PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-347850
(43)Date of publication of application : 15.12.2000

(51)Int.Cl. G06F 9/06
G09C 1/00
G10L 19/00
H03M 7/00
H04L 9/14

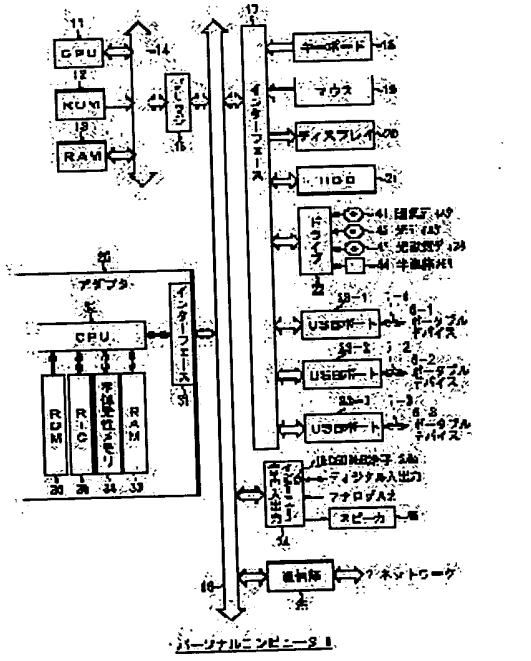
(21)Application number : 2000-087988
(22)Date of filing : 28.03.2000

(71)Applicant : SONY CORP
(72)Inventor : ISHIGURO RYUJI
KAWAKAMI TATSU
TANABE MITSURU
EOMO YUICHI
KAWAHARA HIROKAZU

(30)Priority
Priority number : 11088348 Priority date : 30.03.1999 Priority country : JP

(54) DEVICE AND METHOD FOR INFORMATION PROCESSING AND PROGRAM STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent stored data from illegally being read out and analyzed.
SOLUTION: A CPU 11 rearranges instruction lines included in a program to be executed by an adapter 26. The CPU 11 ciphers the program. On an HDD(Hard Disk Drive) 21, the ciphered program having the instruction lines rearranged is recorded. An interface 17 transmits the program recorded on the HDD 21 to the adapter 26.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application

converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Citation 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－347850
（Ｐ２０００－３４７８５０Ａ）
(43)公開日　平成12年12月15日(2000.12.15)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
G06F 9/06	550	G06F 9/06	550	B
G09C 1/00	660	G09C 1/00	660	D
G10L 19/00		H03M 7/00		
H03M 7/00		G10L 9/00		N
H04L 9/14		H04L 9/00	641	

審査請求　未請求　請求項の数５　ＯＬ　（全48頁）

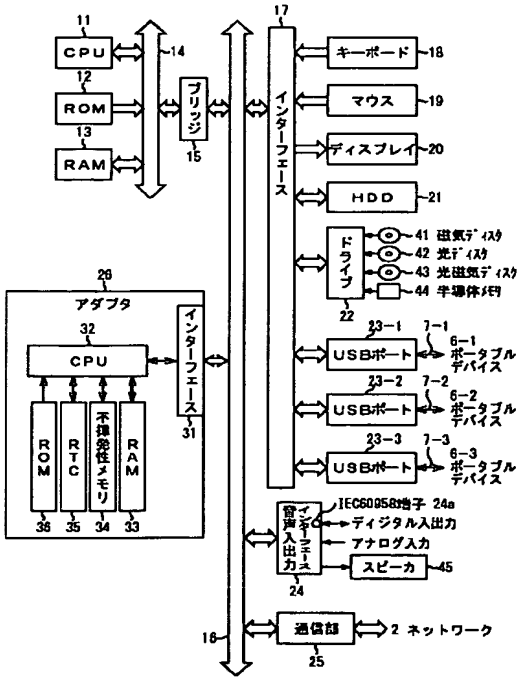
(21)出願番号　特願2000－87988（Ｐ2000－87988）
(22)出願日　平成12年３月28日(2000.3.28)
(31)優先権主張番号　特願平11－88348
(32)優先日　平成11年３月30日(1999.3.30)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　河上　達
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】情報処理装置および方法、並びにプログラム格納媒体

(57)【要約】
【課題】　記憶されているデータが不正に読み出され、解析されるのを防止する。
【解決手段】　CPU１１は、アダプタ２６に実行させるプログラムに含まれる命令列を並び替える。CPU１１は、プログラムを暗号化する。HDD２１は、命令列が並び替えられ、暗号化されたプログラムを記録する。インターフェース１７は、HDD２１に記録されているプログラムを、アダプタ７に送信する。



パーソナルコンピュータ１

1

【特許請求の範囲】

【請求項１】　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置において、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替え手段と、

前記プログラムを暗号化する暗号化手段と、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録手段と、

前記記録手段に記録されている前記プログラムを、前記半導体ＩＣに送信する送信手段とを含むことを特徴とする情報処理装置。

【請求項２】　前記プログラムは、インタープリタに実行させるソースプログラムであることを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記プログラムは、オブジェクトプログラムであることを特徴とする請求項１に記載の情報処理装置。

【請求項４】　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理方法において、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記プログラムを暗号化する暗号化ステップと、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップとを含むことを特徴とする情報処理方法。

【請求項５】　半導体ＩＣが装着され、前記半導体ＩＣに実行させるプログラムを供給する情報処理装置の情報処理用のプログラムであって、

前記半導体ＩＣに実行させる前記プログラムに含まれる命令列を並び替える並び替えステップと、

前記プログラムを暗号化する暗号化ステップと、

前記命令列が並び替えられ、暗号化された前記プログラムを記録する記録ステップと、

前記記録ステップで記録されている前記プログラムを、前記半導体ＩＣに送信する送信ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、所定のデータを記憶し、所定の処理を行う情報処理装置および方法、並びにプログラム格納媒体に関する。

【０００２】

【従来の技術】最近、CD（Compact Disk）、MD（Mini Disk）といった音楽データをデジタル式に記録または再

2

生することができる装置が普及してきた。その結果、このようなデジタル的に音楽データを記録再生できる装置をパーソナルコンピュータなどと組み合わせることで、デジタル音楽データを不正に複製することも比較的容易に行うことができるようになってきた。そこで、著作物としての音楽データを不正に複製することができないようにするために、各種の方法が提案されている。

【０００３】例えば、コピー元を制御するソフトウエアに、コピー先の装置と相互認証させ、適正な認証結果が得られたとき、音楽データを暗号化して、コピー先の装置に転送させ、コピー先の装置において、その暗号化されたデータを復号して利用するようにすることが提案されている。

【０００４】また、コピー元のソフトウエアに所定のハードウエアに記憶されているIDを利用して、コピー先の装置と相互認証させることも提案されている。

【０００５】さらにまた、認証、暗号、および復号処理を、ワイアードロジックのハードウエアで実行させることも提案されている。

【０００６】

【発明が解決しようとする課題】しかしながら、ソフトウエアだけで認証処理、暗号化処理、および復号処理を行うようにする場合、ソフトウエアを解析し、改竄することで、音楽データが不正に複製されてしまう恐れがある。

【０００７】また、所定のIDをハードウエアに記憶させ、パーソナルコンピュータ上のソフトウエアにより、これを読み出し、利用させるようにする場合、読み出されたIDがソフトウエアに転送される途中において読み取られ、解析、改竄されてしまう恐れがあった。

【０００８】さらに、認証処理、暗号化処理、および復号処理をワイアードロジックのハードウエアにより実行するようにすると、解析や改竄は防止することが可能であるが、新たな認証処理、暗号化処理、および復号処理を行うようにするには、既存のハードウエアを新たなハードウエアと交換するか、新たなハードウエアを追加する必要が生じる。

【０００９】本発明はこのような状況に鑑みてなされたものであり、記憶されているデータが不正に読み出され、解析されることを防止できるようにするものである。

【００１０】

【課題を解決するための手段】請求項１に記載の情報処理装置は、半導体ＩＣに実行させるプログラムに含まれる命令列を並び替える並び替え手段と、プログラムを暗号化する暗号化手段と、命令列が並び替えられ、暗号化されたプログラムを記録する記録手段と、記録手段に記録されているプログラムを、半導体ＩＣに送信する送信手段とを含むことを特徴とする。

【００１１】請求項４に記載の情報処理方法は、半導体

ＩＣに実行させるプログラムに含まれる命令列を並び替える並び替えステップと、プログラムを暗号化する暗号化ステップと、命令列が並び替えられ、暗号化されたプログラムを記録する記録ステップと、記録ステップで記録されているプログラムを、半導体ＩＣに送信する送信ステップとを含むことを特徴とする。

【００１２】請求項５に記載のプログラム格納媒体のプログラムは、情報処理装置に、半導体ＩＣに実行させるプログラムに含まれる命令列を並び替える並び替えステップと、プログラムを暗号化する暗号化ステップと、命令列が並び替えられ、暗号化されたプログラムを記録する記録ステップと、記録ステップで記録されているプログラムを、半導体ＩＣに送信する送信ステップとを含むことを特徴とする。

【００１３】請求項１に記載の情報処理装置、請求項４に記載の情報処理方法、および請求項５に記載のプログラム格納媒体においては、半導体ＩＣに実行させるプログラムに含まれる命令列が並び替えられ、プログラムが暗号化され、命令列が並び替えられ、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信される。

【００１４】

【発明の実施の形態】図１は、本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。パーソナルコンピュータ１は、ローカルエリアネットワークまたはインターネットなどから構成されるネットワーク２に接続されている。パーソナルコンピュータ１は、EMD（Elecrical Music Distribution）サーバ４－１乃至４－３から受信した、または後述するCD（Compact Disc）から読み取った楽音のデータ（以下、コンテンツと称する）を、所定の圧縮の方式（例えば、ATRAC3（商標））に変換するとともにDES（Data Encryption Standard）などの暗号化方式で暗号化して記録する。

【００１５】パーソナルコンピュータ１は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【００１６】利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス（Portable Device（PDとも称する））の台数（後述する、いわゆるチェックアウトできるPDの台数）を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ１は、そのコンテンツを再生できる。

【００１７】または、利用条件のデータは、コピーすることができることを示す。コンテンツをポータブルデバイス６－１乃至６－３にコピーしたとき、パーソナルコンピュータ１は記録しているコンテンツを再生できる。コンテンツの、ポータブルデバイス６－１乃至６－３に記憶させることができる回数は、制限される場合がある。この場合、コピーできる回数は、増えることがない。

【００１８】または、利用条件のデータは、他のパーソナルコンピュータに移動することができるなどを示す。ポータブルデバイス６－１乃至６－３にコンテンツを移動させた後、パーソナルコンピュータ１が記録しているコンテンツは使用できなくなる（コンテンツが削除されるか、または利用条件が変更されて使用できなくなる）。

【００１９】利用条件のデータの詳細は、後述する。

【００２０】パーソナルコンピュータ１は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ（例えば、曲名、または再生条件など）と共に、USB（Universal Sirial Bus）ケーブル７－１を介して、接続されているポータブルデバイス６－１に記憶させるとともに、ポータブルデバイス６－１に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する（以下、チェックアウトと称する）。より詳細には、チェックアウトしたとき、パーソナルコンピュータ１が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、１減らされる。チェックアウトできる回数が０のとき、対応するコンテンツは、チェックアウトすることができない。

【００２１】パーソナルコンピュータ１は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USBケーブル７－２を介して、接続されているポータブルデバイス６－２に記憶させるとともに、ポータブルデバイス６－２に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ１は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USBケーブル７－３を介して、接続されているポータブルデバイス６－３に記憶させるとともに、ポータブルデバイス６－３に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

【００２２】また、パーソナルコンピュータ１は、USBケーブル７－１を介して、接続されているポータブルデバイス６－１にパーソナルコンピュータ１がチェックアウトしたコンテンツを、ポータブルデバイス６－１に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する（以下、チェックインと称する）。より詳細には、チェックインしたとき、パーソナルコンピュータ１が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、１増やされる。

【００２３】パーソナルコンピュータ１は、USBケーブル７－２を介して、接続されているポータブルデバイス６－２にパーソナルコンピュータ１がチェックアウトし

たコンテンツを、ポータブルデバイス６－２に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ１は、USBケーブル７－３を介して、接続されているポータブルデバイス６－３にパーソナルコンピュータ１がチェックアウトしたコンテンツを、ポータブルデバイス６－３に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。

【００２４】パーソナルコンピュータ１は、図示せぬ他のパーソナルコンピュータがポータブルデバイス６－１にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ１は、他のパーソナルコンピュータがポータブルデバイス６－２にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ１は、他のパーソナルコンピュータがポータブルデバイス６－３にチェックアウトしたコンテンツをチェックインできない。

【００２５】EMD登録サーバ３は、パーソナルコンピュータ１がEMDサーバ４－１乃至４－３からコンテンツの取得を開始するとき、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、パーソナルコンピュータ１とEMDサーバ４－１乃至４－３との相互認証に必要な認証鍵をパーソナルコンピュータ１に送信するとともに、EMDサーバ４－１乃至４－３に接続するためのプログラムをパーソナルコンピュータ１に送信する。

【００２６】EMDサーバ４－１は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツに関連するデータ（例えば、曲名、または再生制限など）と共に、パーソナルコンピュータ１にコンテンツを供給する。EMDサーバ４－２は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ１にコンテンツを供給する。EMDサーバ４－３は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ１にコンテンツを供給する。

【００２７】EMDサーバ４－１乃至４－３のそれぞれが供給するコンテンツは、同一または異なる圧縮の方式で圧縮されている。EMDサーバ４－１乃至４－３のそれぞれが供給するコンテンツは、同一または異なる暗号化の方式で暗号化されている。

【００２８】WWW（World Wide Web）サーバ５－１は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツを読み取ったCD（例えば、CDのアルバム名、またはCDの販売会社など）、およびCDから読み取ったコンテンツに対応するデータ（例えば、曲名、または作曲者名など）をパーソナルコンピュータ１に供給する。WWWサーバ５－２は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツを読み取ったCD、およびCDから読み取ったコンテンツに対応するデータをパーソナルコンピュータ１に供給する。

【００２９】ポータブルデバイス６－１は、パーソナルコンピュータ１から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、または再生制限など）と共に記憶する。ポータブルデバイス６－１は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

【００３０】例えば、コンテンツに関連するデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス６－１は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス６－１は、対応するコンテンツの再生を停止する。

【００３１】使用者は、コンテンツを記憶したポータブルデバイス６－１をパーソナルコンピュータ１から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【００３２】ポータブルデバイス６－２は、パーソナルコンピュータ１から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス６－２は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス６－２をパーソナルコンピュータ１から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【００３３】ポータブルデバイス６－３は、パーソナルコンピュータ１から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス６－３は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス６－３をパーソナルコンピュータ１から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【００３４】以下、ポータブルデバイス６－１乃至６－３を個々に区別する必要がないとき、単にポータブルデバイス６と称する。

【００３５】図２は、パーソナルコンピュータ１の構成を説明する図である。CPU（CentralProcessing Unit）１１は、各種アプリケーションプログラム（詳細につい

ては後述する）や、OS (Operating System)を実際に実行する。ROM (Read-only Memory) １２は、一般的には、CPU１１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) １３は、CPU１１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス１４により相互に接続されている。

【００３６】ホストバス１４は、ブリッジ１５を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス１６に接続されている。

【００３７】キーボード１８は、CPU１１に各種の指令を入力するとき、使用者により操作される。マウス１９は、ディスプレイ２０の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ２０は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) ２１は、ハードディスクを駆動し、それらにCPU１１によって実行するプログラムや情報を記録または再生させる。

【００３８】ドライブ２２は、装着されている磁気ディスク４１、光ディスク４２ (CDを含む) 、光磁気ディスク４３、または半導体メモリ４４に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース１７、外部バス１６、ブリッジ１５、およびホストバス１４を介して接続されているRAM１３に供給する。

【００３９】USBポート２３－１には、USBケーブル７－１を介して、ポータブルデバイス６－１が接続される。USBポート２３－１は、インターフェース１７、外部バス１６、ブリッジ１５、またはホストバス１４を介して、HDD２１、CPU１１、またはRAM１３から供給されたデータ（例えば、コンテンツまたはポータブルデバイス６－１のコマンドなどを含む）をポータブルデバイス６－１に出力する。

【００４０】USBポート２３－２には、USBケーブル７－２を介して、ポータブルデバイス６－２が接続される。USBポート２３－２は、インターフェース１７、外部バス１６、ブリッジ１５、またはホストバス１４を介して、HDD２１、CPU１１、またはRAM１３から供給されたデータ（例えば、コンテンツまたはポータブルデバイス６－２のコマンドなどを含む）をポータブルデバイス６－２に出力する。

【００４１】USBポート２３－３には、USBケーブル７－３を介して、ポータブルデバイス６－３が接続される。USBポート２３－３は、インターフェース１７、外部バス１６、ブリッジ１５、またはホストバス１４を介して、HDD２１、CPU１１、またはRAM１３から供給されたデータ（例えば、コンテンツまたはポータブルデバイス６－３のコマンドなどを含む）をポータブルデバイス６－３に出力する。

【００４２】IEC (Internationl Electrotechnical Commission) 60958端子２４ａを有する音声入出力インタフェース２４は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ４５は、音声入出力インタフェース２４から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

【００４３】これらのキーボード１８乃至音声入出力インタフェース２４は、インターフェース１７に接続されており、インターフェース１７は、外部バス１６、ブリッジ１５、およびホストバス１４を介してCPU１１に接続されている。

【００４４】通信部２５は、ネットワーク２が接続され、CPU１１、またはHDD２１から供給されたデータ（例えば、登録の要求、またはコンテンツの送信要求など）を、所定の方式のパケットに格納して、ネットワーク２を介して、送信するとともに、ネットワーク２を介して、受信したパケットに格納されているデータ（例えば、認証鍵、またはコンテンツなど）をCPU１１、RAM１３、またはHDD２１に出力する。

【００４５】半導体ICとして、一体的に形成され、パーソナルコンピュータ１に装着されるアダプタ２６のCPU３２は、外部バス１６、ブリッジ１５、およびホストバス１４を介してパーソナルコンピュータ１のCPU１１と共働し、各種の処理を実行する。RAM３３は、CPU３２が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ３４は、パーソナルコンピュータ１の電源がオフされた後も保持する必要があるデータを記憶する。ROM３６には、パーソナルコンピュータ１から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) ３５は、計時動作を実行し、時刻情報を提供する。

【００４６】通信部２５およびアダプタ２６は、外部バス１６、ブリッジ１５、およびホストバス１４を介してCPU１１に接続されている。

【００４７】以下、USBポート２３－１乃至２３－３を個々に区別する必要がないとき、単に、USBポート２３と称する。以下、USBケーブル７－１乃至７－３を個々に区別する必要がないとき、単にUSBケーブル７と称する。

【００４８】次に、ポータブルデバイス６の構成を図３を参照して説明する。電源回路５２は、乾電池５１から供給される電源電圧を所定の電圧の内部電力に変換して、CPU５３乃至表示部６７に供給することにより、ポータブルデバイス６全体を駆動させる。

【００４９】USBコントローラ５７は、USBコネクタ５６を介して、パーソナルコンピュータ１とUSBケーブル７を介して接続された場合、パーソナルコンピュータ１か

ら転送されたコンテンツを含むデータを、内部バス５８を介して、CPU５３に供給する。

【００５０】パーソナルコンピュータ１から転送されるデータは、１パケット当たり64バイトのデータから構成され、12Mbit/secの転送レートでパーソナルコンピュータ１から転送される。

【００５１】ポータブルデバイス６に転送されるデータは、ヘッダおよびコンテンツから構成される。ヘッダには、コンテンツID、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデックID、ファイル情報などが格納されていると共に、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限、および再生回数カウンタなどが格納されている。コンテンツは、ATRAC3などの符号化方式で符号化され、暗号化されている。

【００５２】ヘッダサイズは、ヘッダのデータ長（例えば、33バイトなど）を表し、ファイルサイズは、コンテンツのデータ長（例えば、33,636,138バイトなど）を表す。

【００５３】コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ１とポータブルデバイス６との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ１からポータブルデバイス６に送信される。

【００５４】ポータブルデバイス６がUSBケーブル７を介してパーソナルコンピュータ１のUSBポート２３に接続されたとき、ポータブルデバイス６とパーソナルコンピュータ１とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス６のDSP５９またはCPU５３は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

【００５５】チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ１が生成するある値（チャレンジ）に対して、ポータブルデバイス６がパーソナルコンピュータ１と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ１が生成する値は認証の処理毎に毎回変化するので、例えば、ポータブルデバイス６が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ１は不正を検出できる。

【００５６】コンテンツIDは、コンテンツに対応した、コンテンツを特定するためのIDである。

【００５７】コーデックIDは、コンテンツの符号化方式に対応したIDであり、例えば、コーデックID”１”は、ATRAC3に対応し、コーデックID”０”は、MP3（MPEG(MovingPicture Experts Group) Audio Layer-3）に対応する。

【００５８】ファイル名は、コンテンツに対応するパーソナルコンピュータ１が記録しているコンテンツファイル（後述する）をASCII(American National Standard Codefor Information Interchange)コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、または作曲者名などをASCIIコードに変換したデータである。

【００５９】再生制限データは、コンテンツの再生が可能な期間（すなわち、開始日時または終了日時）または回数制限（再生の回数の制限）が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、”１”が割り当てられ、再生が可能な期間が設定されているとき、”２”が割り当てられ、回数制限および再生が可能な期間がいずれも設定されていないとき（いわゆる、買い取りで購入されたとき）、”０”が割り当てられる。

【００６０】開始日時および終了日時は、再生制限データが”２”であるとき、再生可能期間の範囲を示すデータである。例えば、開始日時が”０００４０Ｆ”であり、終了日時が”０００７０Ｆ”であるとき、対応するコンテンツは、２０００年４月１５日から２０００年７月１５日まで、再生が可能である。

【００６１】同様に、回数制限および再生回数カウンタは、再生制限データが”１”または”２”であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したときCPU５３により更新される、コンテンツが再生された回数を示す。例えば、回数制限が”０２”であるとき、そのコンテンツの再生可能な回数は２回であり、再生回数カウンタが”０１”であるとき、そのコンテンツが再生された回数は１回である。

【００６２】例えば、再生制限データが”２”であり、開始日時が”０００４０Ｆ”であり、終了日時が”０００７０Ｆ”であり、回数制限が”０２”であるとき、ポータブルデバイス６は、対応するコンテンツを、２０００年４月１５日から２０００年７月１５日までの期間において、１日２回ずつ繰り返し再生できる。

【００６３】例えば、再生制限データが”１”であり、開始日時が”０００００”であり、終了日時が”００００００”であり、回数制限が”０ａ”であり、再生回数カウンタが”０５”であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が１０回であり、再生された回数が５回である。

【００６４】ポータブルデバイス６が、パーソナルコンピュータ１からコンテンツと共にコンテンツの書き込み命令を受信した場合、ROM５５からRAM５４に読み出した

メインプログラムを実行するCPU５３は、書き込み命令を受け取り、フラッシュメモリコントローラ６０を制御して、パーソナルコンピュータ１から受信したコンテンツをフラッシュメモリ６１に書き込ませる。

【００６５】フラッシュメモリ６１は、約64MByteの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ６１には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

【００６６】なお、フラッシュメモリ６１は、ポータブルデバイス６にメモリカードとして着脱可能とすることができる。

【００６７】使用者による、図示せぬ再生／停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ６２を介してCPU５３に供給されると、CPU５３は、フラッシュメモリコントローラ６０に、フラッシュメモリ６１から、再生用コードとコンテンツとを読み出させ、DSP５９に転送させる。

【００６８】DSP５９は、フラッシュメモリ６１から転送された再生用コードに基づいてコンテンツをCRC（Cyclic Redundancy Check）方式で誤り検出をした後、再生して、再生したデータ（図３中においてD1で示す）をディジタル／アナログ変換回路６３に供給する。

【００６９】DSP５９は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発信子５９ＡからのマスタークロックMCLKを基に、コンテンツを再生するとともに、マスタークロックMCLK、マスタークロックMCLKを基に内部の発振回路で生成した所定の周波数のビットクロックBCLK、並びにフレーム単位のＬチャンネルクロックLCLK、およびＲチャンネルクロックRCLKからなる動作クロックLRCLKをディジタルアナログ変換回路６３に供給する。

【００７０】DSP５９は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをディジタルアナログ変換回路６３に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、ディジタルアナログ変換回路６３を停止させて、ポータブルデバイス６全体の消費電力量を低減する。

【００７１】同様に、CPU５３およびUSBコントローラ５７も、水晶でなる発振子５３Ａまたは５７Ａがそれぞれ外付けされ、発振子５３Ａまたは５７Ａからそれぞれ供給されるマスタークロックに基づき、所定の処理を実行する。

【００７２】このように構成することで、ポータブルデバイス６は、CPU５３，DSP５９，USBコントローラ５７等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化すると共に小型化することができる。

【００７３】ディジタルアナログ変換回路６３は、再生したコンテンツをアナログの音声信号に変換して、これを増幅回路６４に供給する。増幅回路６４は、音声信号を増幅して、ヘッドフォンジャック６５を介して、図示せぬヘッドフォンに音声信号を供給する。

【００７４】このように、ポータブルデバイス６は、図示せぬ再生／停止ボタンが押圧操作されたとき、CPU５３の制御に基づいてフラッシュメモリ６１に記憶されているコンテンツを再生するとともに、再生中に再生／停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

【００７５】ポータブルデバイス６は、停止後に再度再生／停止ボタンが押圧操作されたとき、CPU５３の制御に基づいて停止した位置からコンテンツの再生を再開する。再生／停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス６は、自動的に電源をオフして消費電力を低減する。

【００７６】因みに、ポータブルデバイス６は、電源がオフになった後に再生／停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、１曲目から再生する。

【００７７】また、ポータブルデバイス６のCPU５３は、LCDコントローラ６８を制御して、表示部６７に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量および乾電池５１の残量等の情報を表示させる。

【００７８】さらに、ポータブルデバイス６は、EEPROM６８に、フラッシュメモリ８０に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ６１のブロック位置、およびその他種々のメモリ蓄積情報等のいわゆるFAT（File Allocation Table）を格納する。

【００７９】因みに、本実施の形態においては、コンテンツは、64KByteを１ブロックとして扱われ、１曲のコンテンツに対応したブロック位置がFATに格納される。

【００８０】フラッシュメモリ６１にFATが格納される場合、例えば、１曲目のコンテンツがCPU５３の制御によりフラッシュメモリ６１に書き込まれると、１曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ６１に書き込まれ、次に、２曲目のコンテンツがフラッシュメモリ６１に書き込まれると、２曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ６１（１曲目と同一の領域）に書き込まれる。

【００８１】このように、FATは、フラッシュメモリ６１へのコンテンツの書き込みの度に書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に２重に書き込まれる。

【００８２】FATがフラッシュメモリ６１に書き込まれると、１回のコンテンツの書き込みに対応して、フラッシュメモリ６１の同一の領域が２回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ６１に規定されている書き換えの回数に達してしまい、フラッシュメモリ６１の書き換えができなくなってしまう。

【００８３】そこで、ポータブルデバイス６は、FATをEEPROM６８に記憶させて、１回のコンテンツの書き込みに対応するフラッシュメモリ６１の書き換えの頻度を少なくしている。

【００８４】書き換えの回数の多いFATをEEPROM６８に記憶させることにより、FATをフラッシュメモリ６１に記憶させる場合に比較して、ポータブルデバイス６は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、CPU５３は、EEPROM６８にFATを追記するように書き込ませるので、EEPROM６８の同一の領域の書き換えの頻度を少なくして、EEPROM６８が短期間で書き換え不能になることを防止する。

【００８５】ポータブルデバイス６は、USBケーブル７を介してパーソナルコンピュータ１に接続されたとき（以下、これをUSB接続と称する）、USBコントローラ５７からCPU５３に供給される割り込み信号に基づき、USB接続されたことを認識する。

【００８６】ポータブルデバイス６は、USB接続されたことを認識すると、パーソナルコンピュータ１からUSBケーブル７を介して規定電流値の外部電力の供給を受けるとともに、電源回路５２を制御して、乾電池５１からの電力の供給を停止させる。

【００８７】CPU５３は、USB接続されたとき、DSP５９のコンテンツの再生の処理を停止させる。これにより、CPU５３は、パーソナルコンピュータ１から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

【００８８】このようにCPU５３は、USB接続されると、乾電池５１から供給される電力からパーソナルコンピュータ１から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ１からの外部電力が使用され、電力単価の高い乾電池５１の消費電力が低減され、かくして乾電池５１の寿命を延ばすことができる。

【００８９】なお、CPU５３は、パーソナルコンピュータ１からUSBケーブル７を介して外部電力の供給を受けたとき、DSP５９の再生処理を停止させることにより、DSP５９からの輻射を低減させ、その結果としてパーソナルコンピュータ１を含むシステム全体の輻射を一段と低減させる。

【００９０】図４は、CPU１１の所定のプログラムの実行等により実現される、パーソナルコンピュータ１の機能の構成を説明するブロック図である。コンテンツ管理プログラム１１１は、EMD選択プログラム１３１、チェックイン／チェックアウト管理プログラム１３２、暗号方式変換プログラム１３５、圧縮方式変換プログラム１３６、暗号化プログラム１３７、利用条件変換プログラム１３９、利用条件管理プログラム１４０、認証プログラム１４１、復号プログラム１４２、PD用ドライバ１４３、購入用プログラム１４４、および購入用プログラム１４５などの複数のプログラムで構成されている。

【００９１】コンテンツ管理プログラム１１１は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム１１１を読み出しても、インストラクションを特定できないなど）ように構成されている。

【００９２】EMD選択プログラム１３１は、コンテンツ管理プログラム１１１がパーソナルコンピュータ１にインストールされるとき、コンテンツ管理プログラム１１１には含まれず、後述するEMDの登録の処理において、ネットワーク２を介して、EMD登録サーバ３から受信される。EMD選択プログラム１３１は、EMDサーバ４－１乃至４－３のいずれかとの接続を選択して、購入用アプリケーション１１５、または購入用プログラム１４４若しくは１４２に、EMDサーバ４－１乃至４－３のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

【００９３】チェックイン／チェックアウト管理プログラム１３２は、チェックインまたはチェックアウトの設定、およびコンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに基づいて、コンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツをポータブルデバイス６－１乃至６－３のいずれかにチェックアウトするか、またはポータブルデバイス６－１乃至６－３に記憶されているコンテンツをチェックインする。

【００９４】チェックイン／チェックアウト管理プログラム１３２は、チェックインまたはチェックアウトの処理に対応して、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに格納されている利用条件のデータを更新する。

【００９５】コピー管理プログラム１３３は、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに基づいて、コンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツをポータブルデバイス６－１乃至６－３のいずれかにコピーするか、またはポータブルデバイス６－１乃至６－３からコンテンツをコンテンツデータベース１１４にコピーする。

【００９６】移動管理プログラム１３４は、コンテンツデータベース１１４に記録されている利用条件ファイル

１６２－１乃至１６２－Ｎに基づいて、コンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツをポータブルデバイス６－１乃至６－３のいずれかに移動するか、またはポータブルデバイス６－１乃至６－３からコンテンツをコンテンツデータベース１１４に移動する。

【００９７】暗号方式変換プログラム１３５は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がEMDサーバ４－１から受信したコンテンツの暗号化の方式、購入用プログラム１４４がEMDサーバ４－２から受信したコンテンツの暗号化の方式、または購入用プログラム１４５がEMDサーバ４－３から受信したコンテンツの暗号化の方式を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツと同一の暗号化の方式に変換する。

【００９８】また、暗号方式変換プログラム１３５は、ポータブルデバイス６－１または６－３にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス６－１または６－３が利用可能な暗号化方式に変換する。

【００９９】圧縮方式変換プログラム１３６は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がEMDサーバ４－１から受信したコンテンツの圧縮の方式、購入用プログラム１４４がEMDサーバ４－２から受信したコンテンツの圧縮の方式、または購入用プログラム１４５がEMDサーバ４－３から受信したコンテンツの圧縮の方式を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツと同一の圧縮の方式に変換する。

【０１００】また、圧縮方式変換プログラム１３６は、ポータブルデバイス６－１または６－３にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス６－１または６－３が利用可能な圧縮の方式に変換する。

【０１０１】暗号化プログラム１３７は、例えばCDから読み取られ、録音プログラム１１３から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツと同一の暗号化の方式で暗号化する。

【０１０２】圧縮／伸張プログラム１３８は、例えばCDから読み取られ、録音プログラム１１３から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム１３８は、符号化されているコンテンツを伸張（復号）する。

【０１０３】利用条件変換プログラム１３９は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がEMDサーバ４－１から受信したコンテンツの利用条件を示すデータ（いわゆる、Usage Rule）、購入用プログラム１４４がEMDサーバ４－２から受信したコンテンツの利用条件を示すデータ、または購入用プログラム１４５がEMDサーバ４－３から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース１１４が記録している利用条件ファイル１６２－１乃至１６２－Ｎに格納されている利用条件データと同一のフォーマットに変換する。

【０１０４】また、利用条件変換プログラム１３９は、ポータブルデバイス６－１または６－３にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス６－１または６－３が利用可能な利用条件のデータに変換する。

【０１０５】利用条件管理プログラム１４０は、コンテンツのコピー、移動、チェックイン、またはチェックアウトの処理を実行する前に、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに格納されている利用条件のデータに対応するハッシュ値（後述する）を基に、利用条件のデータの改竄を検出する。利用条件管理プログラム１４０は、コンテンツのコピー、移動、チェックイン、またはチェックアウトの処理に伴う、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１乃至１６２－Ｎに格納されている利用条件のデータを更新に対応して、利用条件のデータに対応するハッシュ値を更新する。

【０１０６】認証プログラム１４１は、コンテンツ管理プログラム１１１と購入用アプリケーションプログラム１１５との相互認証の処理、およびコンテンツ管理プログラム１１１と購入用プログラム１４４との相互認証の処理を実行する。また、認証プログラム１４１は、EMDサーバ４－１と購入用アプリケーションプログラム１１５との相互認証の処理、EMDサーバ４－２と購入用プログラム１４４との相互認証の処理、およびEMDサーバ４－３と購入用プログラム１４５との相互認証の処理で利用される認証鍵を記憶している。

【０１０７】認証プログラム１４１が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム１１１がパーソナルコンピュータ１にインストールされたとき、認証プログラム１４１に記憶されておらず、表示操作指示プログラム１１２により登録の処理が正常に実行されたとき、EMD登録サーバ３から供給され、認証プログラム１４１に記憶される。

【０１０８】復号プログラム１４２は、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１乃至１６１－Ｎに格納されているコンテンツをパ

ーソナルコンピュータ１が再生するとき、コンテンツを復号する。

【０１０９】PD用ドライバ１４３は、ポータブルデバイス６－２に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス６－２から所定のコンテンツをチェックインするとき、ポータブルデバイス６－２にコンテンツまたはポータブルデバイス６－２に所定の処理を実行させるコマンドを供給する。

【０１１０】PD用ドライバ１４３は、ポータブルデバイス６－１に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス６－１から所定のコンテンツをチェックインするとき、デバイスドライバ１１６－１にコンテンツ、またはデバイスドライバ１１６－１に所定の処理を実行させるコマンドを供給する。

【０１１１】PD用ドライバ１４３は、ポータブルデバイス６－３に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス６－３から所定のコンテンツをチェックインするとき、デバイスドライバ１１６－２にコンテンツ、またはデバイスドライバ１１６－２に所定の処理を実行させるコマンドを供給する。

【０１１２】購入用プログラム１４４は、いわゆる、プラグインプログラムであり、コンテンツ管理プログラム１１１と共にインストールされ、EMD登録サーバ３からネットワーク２を介して供給され、または所定のCDに記録されて供給される。購入用プログラム１４４は、パーソナルコンピュータ１にインストールされたとき、コンテンツ管理プログラム１１１の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム１１１とデータを送受信する。

【０１１３】購入用プログラム１４４は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム１４４を読み出しても、インストラクションを特定できないなど）ように構成されている。

【０１１４】購入用プログラム１４４は、ネットワーク２を介して、EMDサーバ４－２に所定のコンテンツの送信を要求するとともに、EMDサーバ４－２からコンテンツを受信する。また、購入用プログラム１４４は、EMDサーバ４－２からコンテンツを受信するとき、課金の処理を実行する。

【０１１５】購入用プログラム１４５は、コンテンツ管理プログラム１１１と共にインストールされるプログラムであり、ネットワーク２を介して、EMDサーバ４－３に所定のコンテンツの送信を要求するとともに、EMDサーバ４－３からコンテンツを受信する。また、購入用プログラム１４５は、EMDサーバ４－３からコンテンツを受信するとき、課金の処理を実行する。

【０１１６】表示操作指示プログラム１１２は、フィルタリングデータファイル１８１、表示データファイル１８２、画像ファイル１８３－１乃至１８３－K、または履歴データファイル１８４を基に、ディスプレイ２０に所定のウィンドウの画像を表示させ、キーボード１８またはマウス１９への操作を基に、コンテンツ管理プログラム１１１にチェックインまたはチェックアウトなどの処理の実行を指示する。

【０１１７】フィルタリングデータファイル１８１は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１乃至１６１－Nに格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD２１に記録されている。

【０１１８】表示データファイル１８２は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１乃至１６１－Nに格納されているコンテンツに対応するデータを格納して、HDD２１に記録されている。

【０１１９】画像ファイル１８３－１乃至１８３－Kは、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１乃至１６１－Nに対応する画像、または後述するパッケージに対応する画像を格納して、HDD２１に記録されている。

【０１２０】以下、画像ファイル１８３－１乃至１８３－Kを個々に区別する必要がないとき、単に、画像ファイル１８３と称する。

【０１２１】履歴データファイル１８４は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１乃至１６１－Nに格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、HDD２１に記録されている。

【０１２２】表示操作指示プログラム１１２は、登録の処理のとき、ネットワーク２を介して、EMD登録サーバ３に、予め記憶しているコンテンツ管理プログラム１１１のIDを送信するとともに、EMD登録サーバ３から認証用鍵およびEMD選択プログラム１３１を受信して、コンテンツ管理プログラム１１１に認証用鍵およびEMD選択プログラム１３１を供給する。

【０１２３】録音プログラム１１３は、所定のウィンドウの画像を表示させて、キーボード１８またはマウス１９への操作を基に、ドライブ２２に装着された光ディスク４２であるCDからコンテンツの録音時間などのデータを読み出す。

【０１２４】録音プログラム１１３は、CDに記録されているコンテンツの録音時間などを基に、ネットワーク２を介して、WWWサーバ５－１または５－２にCDに対応するデータ（例えば、アルバム名、またはアーティスト名など）またはCDに記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWWサーバ５－１または５－２からCDに対応するデ

ータまたはCDに記録されているコンテンツに対応するデータを受信する。

【０１２５】録音プログラム１１３は、受信したCDに対応するデータまたはCDに記録されているコンテンツに対応するデータを、表示操作指示プログラム１１２に供給する。

【０１２６】また、録音の指示が入力されたとき、録音プログラム１１３は、ドライブ２２に装着された光ディスク４２であるCDからコンテンツを読み出して、コンテンツ管理プログラム１１１に出力する。

【０１２７】コンテンツデータベース１１４は、コンテンツ管理プログラム１１１から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル１６１－１乃至１６１－Ｎのいずれかに格納する（HDD２１に記録する）。コンテンツデータベース１１４は、コンテンツファイル１６１－１乃至１６１－Ｎにそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル１６１－１乃至１６１－Ｎにそれぞれ対応する利用条件ファイル１６２－１乃至１６２－Ｎのいずれかに格納する（HDD２１に記録する）。

【０１２８】コンテンツデータベース１１４は、コンテンツファイル１６１－１乃至１６１－Ｎまたは利用条件ファイル１６２－１乃至１６２－Ｎをレコードとして記録してもよい。

【０１２９】例えば、コンテンツファイル１６１－１に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル１６２－１に格納されている。コンテンツファイル１６１－Ｎに格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル１６２－Ｎに格納されている。

【０１３０】なお、利用条件ファイル１６２－１乃至１６２－Ｎに記録されているデータは、後述する期限データベースに記録されているデータ、または曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース１１４は、後述する期限データベースおよび曲データベースを包含して、構成されている。

【０１３１】以下、コンテンツファイル１６１－１乃至１６１－Ｎを個々に区別する必要がないとき、単に、コンテンツファイル１６１と称する。以下、利用条件ファイル１６２－１乃至１６２－Ｎを個々に区別する必要がないとき、単に、利用条件ファイル１６２と称する。

【０１３２】購入用アプリケーションプログラム１１５は、EMD登録サーバ３からネットワーク２を介して供給され、または所定のCD-ROMに記録されて供給される。購入用アプリケーションプログラム１１５は、ネットワーク２を介して、EMDサーバ４－１に所定のコンテンツの送信を要求するとともに、EMDサーバ４－１からコンテンツを受信して、コンテンツ管理プログラム１１１に供給する。また、購入用アプリケーションプログラム１１５は、EMDサーバ４－１からコンテンツを受信するとき、課金の処理を実行する。

【０１３３】次に、表示データファイル８２に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル１６１－１乃至１６１－Ｎとの対応付けについて説明する。

【０１３４】コンテンツファイル１６１－１乃至１６１－Ｎのいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、またはフィルタリングパッケージのいずれかである。

【０１３５】オリジナルパッケージは、１以上のコンテンツが属し、EMDサーバ４－１乃至４－３におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、または一枚のCDに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、または追加した情報の変更）することができる。

【０１３６】マイセレクトパッケージは、使用者が任意に選択した１以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、１以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

【０１３７】フィルタリングパッケージには、フィルタリングデータファイル１８１に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、EMDサーバ４－１乃至４－３またはWWWサーバ５－１若しくは５－２などからネットワーク２を介して供給され、または所定のCDに記録されて供給される。使用者は、フィルタリングデータファイル１８１に格納されているフィルタリングデータを編集することができる。

【０１３８】フィルタリングデータは、所定のコンテンツを選択する、またはコンテンツに対応する重みを算出する基準となる。例えば、今週のＪ－ＰＯＰ（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ１は、今週の日本のポップス１位のコンテンツ乃至今週の日本のポップス１０位のコンテンツを特定することができる。

【０１３９】フィルタリングデータファイル１８１は、例えば、過去１月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、または曲名に”愛”の文字が含まれているコンテンツを選択するフィル

タリングデータなどを含んでいる。

【０１４０】このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ２２１（コンテンツ用表示データ２２１に使用者が設定したデータを含む）、または履歴データ１８４などと、フィルタリングデータとを対応させて選択される。

【０１４１】ドライバ１１７は、コンテンツ管理プログラム１１１などの制御の基に、音声入出力インターフェース２４を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム１１１に供給するか、若しくはコンテンツ管理プログラム１１１を介してコンテンツデータベース１１４から供給されたコンテンツをデジタルデータとして出力するか、または、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４から供給されたコンテンツに対応するアナログ信号を出力する。

【０１４２】図５は、表示操作指示プログラム１１２を起動させたとき、操作指示プログラム１１２がディスプレイ２０に表示させる表示操作指示ウィンドウの例を示す図である。

【０１４３】表示操作指示ウィンドウには、録音プログラム１１３を起動させるためのボタン２０１、EMD選択プログラム１３１を起動させるためのボタン２０２、チェックインまたはチェックアウトの処理の設定を行うフィールドを表示させるためのボタン２０３、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン２０４等が配置されている。

【０１４４】ボタン２０５が選択されているとき、フィールド２１１には、オリジナルパッケージに対応するデータが表示される。ボタン２０６が選択されているとき、フィールド２１１には、マイセレクトパッケージに対応するデータが表示される。ボタン２０７が選択されているとき、フィールド２１１には、フィルタリングパッケージに対応するデータが表示される。

【０１４５】フィールド２１１に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、またはアーティスト名などである。

【０１４６】例えば、図５においては、パッケージ名称”ファースト”およびアーティスト名”Ａ太郎”、およびパッケージ名称”セカンド”およびアーティスト名”Ａ太郎”などがフィールド２１１に表示される。

【０１４７】フィールド２１２には、フィールド２１１で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド２１２に表示されるデータは、例えば、曲名、演奏時間、またはチェックアウト可能回数などである。

【０１４８】例えば、図５においては、パッケージ名称”セカンド”に対応するパッケージが選択されているので、パッケージ名称”セカンド”に対応するパッケージに属するコンテンツに対応する曲名”南の酒場”およびチェックアウト可能回数（例えば、８分音符の１つがチェックアウト１回に相当し、８分音符が２つでチェックアウト２回を示す）、並びに曲名”北の墓場”およびチェックアウト可能回数（８分音符が１つでチェックアウト１回を示す）などがフィールド２１２に表示される。

【０１４９】このように、フィールド２１２に表示されるチェックアウト可能回数としての１つの８分音符は、対応するコンテンツが１回チェックアウトできることを示す。

【０１５０】フィールド２１２に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が０である。（ただし、パーソナルコンピュータ１はそのコンテンツを再生することができる。））ことを示す。また、フィールド２１２に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限が無い（何度でも、チェックアウトできる）ことを示している。

【０１５１】なお、チェックアウト可能回数は、図５に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等で表示してもよい。

【０１５２】また、表示操作指示ウィンドウには、選択されているパッケージまたはコンテンツに対応付けられている画像等（図４の画像ファイル１８３－１乃至１８３－Ｋのいずれかに対応する）を表示させるフィールド２０８が配置されている。ボタン２０９は、選択されているコンテンツを再生する（コンテンツに対応する音声をスピーカ４５に出力させる）とき、クリックされる。

【０１５３】ボタン２０５が選択され、フィールド２１１に、オリジナルパッケージに対応するデータが表示されている場合、フィールド２１２に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１に、選択されている曲名に対応する、コンテンツデータベース１１４に格納されている所定のコンテンツを消去させる。

【０１５４】録音プログラム１１３が表示させるウィンドウのボタン（後述するボタン２５５）が選択されて（アクティブにされて）いる場合、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス６－１乃至６－３のいずれかに記憶されているコンテンツの曲名を表示するフィールド２１３を表示する。

【０１５５】録音プログラム１１３が表示させるウィンドウのボタンが選択されている場合、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、表示操作指示プログラム１１２は、コンテン

ツ管理プログラム１１１に、コンテンツデータベース１１４に記録した、ＣＤから読み出したコンテンツを予め指定されているポータブルデバイス６－１乃至６－３のいずれかにチェックアウトさせる。

【０１５６】フィールド２１３にはコンテンツの曲名に対応させて、フィールド２１３の最も左に、そのコンテンツがパーソナルコンピュータ１にチェックインできるか否かを示す記号が表示される。例えば、フィールド２１３の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ１にチェックインできる（すなわち、パーソナルコンピュータ１からチェックアウトされた）ことを示している。フィールド２１３の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ１にチェックインできない（すなわち、パーソナルコンピュータ１からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

【０１５７】表示操作指示プログラム１１２が表示操作指示ウィンドウにフィールド２１３を表示させたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス６－１乃至６－３のいずれかに記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス６－１乃至６－３のいずれかに記憶されているコンテンツが属するパーケージ）の名称を表示するフィールド２１４、フィールド２１３を閉じるためのボタン２１０、およびチェックインまたはチェックアウトを実行させるボタン２１５を表示する。

【０１５８】更に、表示操作指示プログラム１１２が表示操作指示ウィンドウにフィールド２１３を表示させたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、フィールド２１２で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン２１６、フィールド２１３で選択された曲名に対応するコンテンツのチェックインを設定するボタン２１７、フィールド２１３に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン２１８、およびチェックインまたはチェックアウトの設定を取り消すボタン２１９を配置させる。

【０１５９】ボタン２１６乃至２１９の操作によるチェックインまたはチェックアウトの設定だけでは、パーソナルコンピュータ１は、チェックインまたはチェックアウトの処理を実行しない。

【０１６０】ボタン２１６乃至２１９の操作によるチェックインまたはチェックアウトの設定をした後、ボタン２１５がクリックされたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１にチェックインまたはチェックアウトの処理を実行させる。すなわち、ボタン２１５がクリックされたとき、表示操作指示

プログラム１１２は、チェックインまたはチェックアウトの設定に基づき、コンテンツ管理プログラム１１１に、ポータブルデバイス６－１乃至６－３のいずれかにコンテンツを送信させるか、またはチェックインに対応する所定のコマンド（例えば、ポータブルデバイス６－１乃至６－３のいずれかが記憶している所定のコンテンツを消去させるコマンドなど）を送信させるとともに、送信したコンテンツまたはコマンドに対応する利用条件ファイル１６２に格納されている利用条件のデータを更新させる。

【０１６１】チェックインまたはチェックアウトが実行されたとき、表示操作指示プログラム１１２は、送信したコンテンツまたは送信されたコマンドに対応して、履歴データファイル１８４に格納されている履歴データを更新する。履歴データは、チェックインまたはチェックアウトされたコンテンツを特定する情報、またはそのコンテンツがチェックインまたはチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス６－１乃至６－３の名称などから成る。

【０１６２】チェックインまたはチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックインまたはチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックインまたはチェックアウトの処理の回数を減らして、チェックインまたはチェックアウトに必要な時間全体（設定および実行を含む）を短くすることができる。

【０１６３】図６は、録音プログラム１１３がディスプレイ２０に表示させるウィンドウの例を説明する図である。例えば、WWWサーバ５－２から受信したCDの情報を基に、録音プログラム１１３は、フィールド２５１に、”アシンクロナイズド”などのCDのタイトルを表示する。WWWサーバ５－２から受信したCDの情報を基に、録音プログラム１１３は、フィールド２５２に、例えば、”クワイ”などのアーティスト名を表示する。

【０１６４】WWWサーバ５－２から受信したCDの情報を基に、録音プログラム１１３は、フィールド２５３の曲名を表示する部分に、例えば、”ヒート”，”プラネット”，”ブラック”，”ソウル”などの曲名を表示する。同様に、録音プログラム１１３は、フィールド２５３のアーティストを表示する部分に、例えば、”クワイ”などのアーティスト名を表示する。

【０１６５】録音プログラム１１３が所定のCDの情報を受信した後、録音プログラム１１３は、HDD２１の所定のディレクトリにCDの情報を格納する。

【０１６６】ボタン２５４などがクリックされて、CDの情報の取得の指示を受けたとき、録音プログラム１１３は、始めに、HDD２１の所定のディレクトリを検索する。録音プログラム１１３は、そのディレクトリにCDの情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されている

CDの情報を利用するか否かを選択させる。

【０１６７】録音プログラム１１３が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン２５６がクリックされたとき、録音プログラム１１３は、ドライブ２２に格納されているCDからコンテンツを読み出して、CDから読み出したコンテンツをCDの情報と共にコンテンツ管理プログラム１１１に供給する。コンテンツ管理プログラム１１１の圧縮／伸張プログラム１３８は、録音プログラム１１３から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム１３７は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム１３９は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

【０１６８】コンテンツ管理プログラム１１１は、圧縮され、暗号化されたコンテンツを利用条件のデータと共に、コンテンツデータベース１１４に供給する。

【０１６９】コンテンツデータベース１１４は、コンテンツ管理プログラム１１１から受信したコンテンツに対応するコンテンツファイル１６１および利用条件ファイル１６２を生成して、コンテンツファイル１６１にコンテンツを格納するとともに、利用条件ファイル１６２に利用条件のデータを格納する。

【０１７０】コンテンツ管理プログラム１１１は、コンテンツデータベース１１４にコンテンツおよびコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム１１３から受信したCDの情報および利用条件のデータを表示操作指示プログラム１１２に供給する。

【０１７１】表示操作指示プログラム１１２は、録音の処理でコンテンツデータベース１１４に格納されたコンテンツに対応する利用条件のデータおよびCDの情報を基に、表示データファイル１８２に格納する表示用のデータを生成する。

【０１７２】録音プログラム１１３が表示させるウィンドウには、更に、CDから読み出したコンテンツをコンテンツデータベース１１４に記録したとき、自動的に、CDから読み出したコンテンツをポータブルデバイス６－１乃至６－３のいずれかにチェックアウトさせるか否かの設定を行うボタン２５５が配置されている。

【０１７３】例えば、ボタン２５５がクリックされたとき、録音プログラム１１３は、ポータブルデバイス６－１乃至６－３のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス６－１乃至６－３のいずれかを選択したとき、パーソナルコンピュータ１は、選択されたポータブルデバイス６－１乃至６－３のいずれかに、自動的に、CDから記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから”チェックアウトしない”を選択した場合、パーソナルコンピュータ１は、CDからコンテンツを記録したとき、チェックアウトしない。

【０１７４】このように、録音プログラム１１３が表示させるウィンドウのボタン２５５をアクティブにしておくだけで、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、パーソナルコンピュータ１は、予め指定されているポータブルデバイス６－１乃至６－３のいずれかに、ＣＤから読み出したコンテンツをチェックアウトさせることができる。

【０１７５】次に、図７のフローチャートを参照して、コンテンツ管理プログラム１１１、表示操作指示プログラム１１２、録音プログラム１１３、およびコンテンツデータベース１１４を実行するCPU１１による、ドライブ２２に装着されたCDから再生したコンテンツをHDD２１に転送し、コピーする場合の処理について説明する。使用者がキーボード１８またはマウス１９を操作して、インタフェース１７を介してCPU１１に対してドライブ２２に装着されたCD（図示せず）から再生されたコンテンツをHDD２１に転送、コピーする指令を入力すると、録音プログラム１１３は、ステップＳ１１において、インタフェース１７を介してディスプレイ２０にコピーするコンテンツを選択するための、例えば、図６に示すGUI（Graphical User Interface）を表示させる。

【０１７６】具体的には、例えば、録音プログラム１１３は、ドライブ２２に装着されたCDのTOC（Table Of Contents）を読み込み、そのCDに含まれるコンテンツの情報を得て、ディスプレイ２０に表示させる。または、録音プログラム１１３は、CDに含まれている各コンテンツ毎のISRC（International Standard Recording Code）を読み出し、そのコンテンツの情報を得て、ディスプレイ２０に表示させる。あるいはまた、ボタン２５４がクリックされたとき、録音プログラム１１３は、ネットワーク２を介してWWWサーバ５－１または５－２にアクセスし、TOCを用いて、そのCDのコンテンツの情報を得て、コンテンツに対応する曲名などをフィールド２５３に表示させる。

【０１７７】使用者は、ディスプレイ２０のGUIを利用してキーボード１８またはマウス１９を操作し、フィールド２５３に表示されている曲名に対応するチェックボックスをクリックするなどして、コピーするコンテンツを選択する。

【０１７８】次に、ステップＳ１２において、録音プログラム１１３は、利用条件管理プログラム１４０に、HDD２１に格納されている期限データベース（図４に示すコンテンツデータベース１１４の利用条件ファイル１６２－１乃至１６２－Ｎに対応する）をチェックさせる。この期限データベースチェック処理の詳細は、図８のフローチャートに示されている。

【０１７９】ステップＳ３１において利用条件管理プログラム１４０は、アダプタ２６のCPU３２と共働して、期限データベース全体のハッシュ値を計算し、ステップ

Ｓ３２において、その計算された値と、前回保存しておいたハッシュ値と比較する。

【０１８０】なお、期限データベースにデータが何ら記録されていないとき、利用条件管理プログラム１４０は、ハッシュ値を計算しない。

【０１８１】すなわち、HDD２１には、期限データベースが形成されており、この期限データベースには、図９に示すように、HDD２１に記録されているコンテンツ（コンテンツ）を管理する管理情報として、過去に記録されたことのあるコンテンツのISRCとコピー日時が対応して記憶されている。この例においては、アイテム１乃至アイテム３の３つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全てのコンテンツのISRCとコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップＳ３８において、アダプタ２６のCPU３２により計算され、不揮発性メモリ３４に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。

【０１８２】ハッシュ関数は、任意の長さのメッセージを固定長に短く圧縮した値にマップする一方向性の関数であり、圧縮したデータからもとのデータを求める逆変換が困難な性質を持つものである。また、ハッシュ値同士の衝突が起こりにくく、即ち、例えば違う二つのメッセージに対して同じ値を付けることを困難にするものである。ハッシュ関数は、メッセージが通信途中で改竄されなかったことを確証するためのチェックサムとして用いられたり、ディジタル署名の中で用いられたりする。ハッシュ関数の例としては、SHA (Secure Hash Algorithm)，MD (Message Digest) ５などがある。

【０１８３】利用条件管理プログラム１４０は、ステップＳ３１において、CPU３２が実行したのと同様にハッシュ値を計算する。そして、ステップＳ３２において、利用条件管理プログラム１４０は、CPU３２に、不揮発性メモリ３４に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップＳ３１で、いま自分自身が計算したハッシュ値とを比較する。

【０１８４】ステップＳ３３において、利用条件管理プログラム１４０は、ステップＳ３１でいま計算したハッシュ値と、不揮発性メモリ３４に記憶されている前回の期限データベースのハッシュ値とが一致するか否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、利用条件管理プログラム１４０は、ステップＳ３４において、例えば、録音プログラム１１３に「期限データベースが改竄されたので、コピーができません」といったメッセージを発生させ、インタフェース１７を介してディスプレイ２０に出力させ、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されているコンテンツを再生し、HDD２１にコピーする処理が禁止される。

【０１８５】ステップＳ３１で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップＳ３５に進み、利用条件管理プログラム１４０は、録音プログラム１１３に、ステップＳ１１で指定されたコピーするコンテンツとして選択されたコンテンツ（選択されたコンテンツ）のISRCをCDから取得させる。CDにISRCが記録されていない場合、利用条件管理プログラム１４０は、録音プログラム１１３に、そのCDのTOCのデータを読み出させ、そのデータにハッシュ関数を適用するなどして、例えば、５８ビットなどの適当な長さのデータを得て、これをISRCに代えて用いる。

【０１８６】ステップＳ３６において、利用条件管理プログラム１４０は、ステップＳ３５で取得したISRC（すなわち、選択されたコンテンツ）が期限データベース（図９）に登録されているか否かを判定する。ISRCが期限データベースに登録されていない場合には、そのコンテンツはまだHDD２１に記録されていないことになるので、ステップＳ３７に進み、利用条件管理プログラム１４０は、そのコンテンツのISRCと現在の日時とを期限データベースに登録する。なお、利用条件管理プログラム１４０は、この現在の日時として、CPU３２から転送を受けた、アダプタ２６のRTC３５が出力する値を利用する。そして、ステップＳ３８において、利用条件管理プログラム１４０は、その時点における期限データベースのデータを読み出し、アダプタ２６のCPU３２に転送する。CPU３２は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ３４に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップＳ３２において、前回保存しておいたハッシュ値として利用される。

【０１８７】次に、ステップＳ３９において、利用条件管理プログラム１４０は、選択されたコンテンツが期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図７のステップＳ１３において、選択されたコンテンツが期限データベースに登録されているか否かの判定を行うときに用いられる。

【０１８８】ステップＳ３６において、選択されたコンテンツのISRCが期限データベースに登録されていると判定された場合、その選択されたコンテンツは、少なくとも一度、HDD２１に登録されたことがあるコンテンツであるということになる。そこで、この場合、ステップＳ４０に進み、利用条件管理プログラム１４０は、期限データベースに登録されているその選択されたコンテンツの登録日時より、現在の日時（アダプタ２６のRTC３５が出力した現在の日時）が４８時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に４８時間以上経過している場合には、HDD２１に、少なくとも一度は記録したことがあるが、既に、その時から４８時間以上経過しているので、そのコンテンツを再度コピ

ーさせたとしても、コンテンツの大量のコピーは実質的に不可能なので、この場合には、HDD２１へのコピーが許容される。そこで、ステップＳ４１に進み、利用条件管理プログラム１４０は、期限データベースの日時を、過去の登録日時から現在の日時（RTC３５の出力する日時）に変更させる。そして、ステップＳ３８に戻り、利用条件管理プログラム１４０は、再び、期限データベース全体のハッシュ値をCPU３２に計算させ、不揮発性メモリ３４に保存させるとともに、ステップＳ３９において、そのコンテンツに対して未登録のフラグを設定する。

【０１８９】一方、ステップＳ４０において、現在時刻が登録日時より、まだ４８時間以上経過していないと判定された場合、その選択されたコンテンツのHDD２１へのコピーが禁止される。そこで、この場合には、ステップＳ４２に進み、利用条件管理プログラム１４０は、その選択されたコンテンツに対応して登録済みのフラグを設定する。

【０１９０】ステップＳ４０の処理により、所定の時間が経過しなければ、コンテンツの新たなコピーを生成できないので、不正でない通常の使用を目的としたコンテンツのコピーの生成を不当に妨げることなく、例えば、不正な販売または配布などに必要な大量のコンテンツのコピーの生成は、実質的に不可能となる。なお、ステップＳ４０においては、判定の基準は４８時間以上の経過としたが、４８時間に限らず、例えば、１２時間乃至１６８時間のいずれかの時間であればよい。

【０１９１】以上のようにして、期限データベースチェック処理により、選択されたコンテンツがHDD２１に登録されているか否かを表すフラグが設定される。

【０１９２】図７に戻り、ステップＳ１３においてコピー管理プログラム１３３は、選択されたコンテンツが期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択されたコンテンツが登録済みである場合には、ステップＳ１４に進み、コピー管理プログラム１３３は、録音プログラム１１３に、例えば、「この曲は一度コピーされてからまだ４８時間以上経過していないので、コピーすることができません」のようなメッセージをディスプレイ２０に表示させる。これにより、使用者は、そのコンテンツをHDD２１にコピーすることができない理由を知ることができる。

【０１９３】ステップＳ１３において、選択したコンテンツが期限データベースに登録されていないと判定された場合、ステップＳ１５に進み、録音プログラム１１３は、ドライブ２２を制御し、そこに装着されているCDからコンテンツを読み出させる。このコンテンツには、図１０に示すように、所定の位置にウォータマークコードが挿入されている。録音プログラム１１３は、ステップＳ１６において、コンテンツに含まれているウォータマークコードを抽出し、そのウォータマークコードがコピー禁止を表しているいるか否かをステップＳ１７において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップＳ１８に進み、コピー管理プログラム１３３は、録音プログラム１１３に例えば、「コピーは禁止されています」のようなメッセージをインタフェース１７を介してディスプレイ２０に表示させ、コピー処理を終了させる。

【０１９４】これに対して、ステップＳ１７において、ウォータマークがコピー禁止を表していないと判定された場合、ステップＳ１９に進み、録音プログラム１１３は、コンテンツを、圧縮／伸張プログラム１３８に、例えば、ATRAC（Adaptive Transform Acoustic Coding）３（商標）などの方式で、ソフトウェア処理により圧縮させる。ステップＳ２０において、録音プログラム１１３は、暗号化プログラム１３７に、予め設定され、メモリ１３に記憶されている暗号鍵を用いて、例えば、DES（Data Encryption Standard）方式、FEAL（Fast Encripherment Algotithm）方式などの暗号化方法により、コンテンツを暗号化させる。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ２６のCPU３２により発生させた乱数に基づいて生成したものを用いることもできる。このように、パーソナルコンピュータ１だけではなく、それに付随して装着されたハードウェアとしてのアダプタ２６のCPU３２と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

【０１９５】次に、ステップＳ２１において、録音プログラム１１３は、暗号化されたデータを、コンテンツデータベース１１４に転送し、１つのファイル（コンテンツファイル１６１として）としてファイル名を付けてHDD21に保存させる。あるいはまた、１つのファイルの一部として、そのファイル名の位置情報（例えば、先頭からのバイト数）を与えて保存するようにしてもよい。

【０１９６】この保存処理と、上記した圧縮符号化処理および暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

【０１９７】さらに、ステップＳ２２において、録音プログラム１１３は、暗号化プログラム１３７に、予め定められている不揮発性メモリ３４に記憶されている保存用鍵を使って、上述したDES方式、FEAL方式などの方式で、コンテンツを暗号化した暗号鍵を暗号化させ、HDD２１の曲データベース（図４に示すコンテンツデータベース１１４の利用条件ファイル１６２－１乃至１６２－Ｎに対応する）に保存する。

【０１９８】ステップＳ２３において、録音プログラム１１３は、保存したファイルに関する情報、暗号化された暗号鍵、そのコンテンツの情報、使用者がGUIを介して入力した曲名の情報の要素を組にしてHDD２１の曲データベースに登録する（利用条件ファイル１６２－１乃至１６２－Ｎとして記録する）。そして、ステップＳ２

４において、録音プログラム１１３は、CPU３２に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ３４に保存させる。

【０１９９】このようにして、例えば、図１１に示すような曲データベースが、HDD２１上に登録される。この例においては、アイテム１乃至アイテム３のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ、およびコピー条件（SCMS）が記録されている。

【０２００】例えば、SDMI（Secure Digital Music Initiative）が規定する方式では、CDからコピーしたコンテンツに対応して、そのコンテンツがチェックアウトできる回数は、３回に設定される。

【０２０１】CDからHDD２１にコンテンツが複製されて一定期間が経過すると、再びコンテンツを複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとすると、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ１が故障して、HDD２１に記録されていたコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、HDD２１に記録することができる。

【０２０２】また、例えば、ネットワーク２を介してHDD２１に記録されている期限データベースの内容を共有することもできる。

【０２０３】以上においては、ISRCに対応して複製された日時が記憶されている場合を例として説明したが、コンテンツやCDを識別する情報であれば、他のもの（例えば、曲名、アルバム名、それらの組み合わせなど）を利用することもできる。

【０２０４】次に、図１２乃至図１４のフローチャートを参照して、表示操作指示プログラム１１２およびコンテンツ管理プログラム１１１を実行するCPU１１およびメインプログラムを実行するCPU５２による、HDD２１からポータブルデバイス６のフラッシュメモリ６１（例えば、メモリースティック（商標））に、コンテンツを移動する処理およびチェックアウトの処理について説明する。

【０２０５】始めに、コンテンツの移動の処理について説明する。ステップＳ５１において、移動管理プログラム１３４は、利用条件管理プログラム１４０に、曲データベース全体のハッシュ値を計算させ、ステップＳ５２で、前回CPU３２に計算させ、不揮発性メモリ３４に保存しておいたハッシュ値と比較する。両者が一致しない場合、移動管理プログラム１３４は、ステップＳ５３に進み、表示操作指示プログラム１１２に、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ２０に表示させた後、処理を終了させる。この場合の処理は、図８のステップＳ３１乃至ステップＳ３４の処理と同様の処理である。この場合においては、HDD２１からポータブルデバイス６へのコンテンツの移動が実行されないことになる。

【０２０６】次に、ステップＳ５４において、移動管理プログラム１３４は、HDD２１に形成されている曲データベース（コンテンツデータベース１１４に含まれる）から、そこに登録されているコンテンツの情報を読み出し、表示操作指示プログラム１１２に、選択のためのGUIとしてディスプレイ２０に表示させる。使用者は、この選択のためのGUIに基づいて、HDD２１からポータブルデバイス６へ移動させるコンテンツを、図５のフィールド２１２に表示される曲名、ボタン２１６などをクリックして選択する。次に、ステップＳ５５において、移動管理プログラム１３４は、ステップＳ５４で選択された選択されたコンテンツの再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図１５のフローチャートを参照して後述する。

【０２０７】次に、ステップＳ５６において、パーソナルコンピュータ１の認証プログラム１４１とポータブルデバイス６のCPU５３との間において、相互認証処理が行われ、通信用鍵が共有される。

【０２０８】例えば、ポータブルデバイス６のフラッシュメモリ６１（または、EEPROM６８）には、マスター鍵KMMが予め記憶されており、パーソナルコンピュータ１のRAM１３（または、HDD２１の所定のファイル）には、個別鍵KPPとIDが予め記憶されているものとする。CPU５３は、認証プログラム１４１から、RAM１３に予め記憶されているIDの供給を受け、そのIDと自分自身が有するマスター鍵KMMにハッシュ関数を適用して、RAM１３に記憶されているパーソナルコンピュータ１の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ１とポータブルデバイス６の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

【０２０９】あるいはまた、パーソナルコンピュータ１のRAM１３にIDとマスター鍵KMPを予め記憶させておくとともに、ポータブルデバイス６のフラッシュメモリ６１にもポータブルデバイス６のIDと個別鍵KPMを記憶させておく。そして、それぞれのIDとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたIDとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

【０２１０】なお、認証の方法としては、例えば、IOS（International Organization forStandardization）９７９８－２を利用することができる。

【０２１１】相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップＳ５７において、移動管理プログラム１３４は、コ

ンテンツデータベース１１４に、選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツ（例えば、図７のステップＳ２０の処理で暗号化されている）をHDD２１から読み出す。ステップＳ５８において、移動管理プログラム１３４は、ステップＳ５７で読み出したデジタルデータであるコンテンツの圧縮符号化方式（ステップＳ１９の処理）、暗号化方式（ステップＳ２０の処理）、フォーマット（例えば、ヘッダの方式など）などをポータブルデバイス６のものに変換する処理を実行する。この変換処理の詳細は、図１７のフローチャートを参照して後述する。

【０２１２】ステップＳ５９において、移動管理プログラム１３４は、PD用ドライバ１４３に、ステップＳ５８で変換したコンテンツを、USBポート２３を介してポータブルデバイス６に転送させる。ステップＳ６０において、ポータブルデバイス６のCPU５３は、USBコネクタ５６を介してこの伝送されてきたコンテンツを受信すると、そのコンテンツを、そのままフラッシュメモリ６１に記憶させる。

【０２１３】ステップＳ６１において、移動管理プログラム１３４は、さらに、利用条件変換プログラム１３９に、曲データベースに登録されているその選択されたコンテンツの再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス６が管理している形式に変換する。ステップＳ６２において、移動管理プログラム１３４は、さらに、利用条件変換プログラム１３９に、選択されたコンテンツの曲データベース中に登録されているコピー条件中のSCMS情報を、ポータブルデバイス６の管理する形式に変換させる。そして、ステップＳ６３において、移動管理プログラム１３４は、PD用ドライバ１４３に、ステップＳ６１で変換した再生条件と、ステップＳ６２で変換したSCMS情報を、ポータブルデバイス６に転送させる。ポータブルデバイス６のCPU５３は、転送を受けた再生条件とSCMS情報を、フラッシュメモリ６１に保存する。

【０２１４】ステップＳ６４において、移動管理プログラム１３４はまた、PD用ドライバ１４３に、選択されたコンテンツの曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU１１が曲データベース中で扱っている形式のまま、ポータブルデバイス６に転送させ、フラッシュメモリ６１に保存させる。

【０２１５】ステップＳ６５において、移動管理プログラム１３４は、コンテンツデータベース１１４に、選択されたコンテンツの暗号化されている暗号鍵を曲データベースから読み出させ、ステップＳ６６において、復号プログラム１４２に、その暗号鍵をRAM１３に保存されている保存用鍵で復号させ、暗号化プログラム１３７に通信用鍵で暗号化させる。そして、通信用鍵で暗号化した暗号鍵を、移動管理プログラム１３４は、PD用ドライバ１４３に、ポータブルデバイス６へ転送させる。

【０２１６】ポータブルデバイス６のCPU５３は、ステップＳ６７で、パーソナルコンピュータ１から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ６１に保存する。

【０２１７】CPU５３は、暗号鍵の保存が完了すると、ステップＳ６８において、パーソナルコンピュータ１に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ１の移動管理プログラム１３４は、ポータブルデバイス６からこの通知を受けると、ステップＳ６９において、コンテンツデータベース１１４に、そのコンテンツに対応するコンテンツファイル１６１を削除させるとともに、曲データベースからそのコンテンツの要素の組（すなわち、利用条件ファイル１６２）を削除させる。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップＳ７０において、移動管理プログラム１３４は、アダプタ２６のCPU３２に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ３４に保存させる。このハッシュ値が、上述したステップＳ５２において、前回保存しておいたハッシュ値として用いられることになる。

【０２１８】次に、パーソナルコンピュータ１からポータブルデバイス６にコンテンツをチェックアウトする処理について説明する。パーソナルコンピュータ１からポータブルデバイス６にコンテンツをチェックアウトする処理は、図１２乃至図１４のパーソナルコンピュータ１からポータブルデバイス６へコンテンツを移動させる場合と同様の処理である。すなわち、チェックアウトの処理は、パーソナルコンピュータ１においてチェックイン／チェックアウト管理プログラム１３２により実行され、図１４のステップＳ６９において、コンテンツを削除する処理に代えて、曲データベースに記録されている、チェックアウトされたコンテンツのチェックアウトした回数（またはチェックアウトできる回数）を更新する処理を実行することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

【０２１９】次に、コンテンツ管理プログラム１１１を実行するCPU１１による、図１２のステップＳ５５における選択されたコンテンツの再生条件などのチェック処理について図１５のフローチャートを参照して説明する。ステップＳ８１において、移動管理プログラム１３４は、コンテンツデータベース１１４に、曲データベースから、各種の条件を読み出させる。移動管理プログラム１３４は、ステップＳ８２において、ステップＳ８１で読み出した各種条件のうち、コピー回数がコピー制限

回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップＳ８３に進み、移動管理プログラム１３４は、表示操作指示プログラム１１２に、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ２０に表示させ、処理を終了させる。ステップＳ８２において、コピー回数がコピー制限回数を過ぎていないと判定された場合、ステップＳ８４に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ２６のRTC３５より出力されたものが用いられる。これにより、使用者が、パーソナルコンピュータ１の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。移動管理プログラム１３４は、この現在日時をCPU３２から提供を受けて、ステップＳ８４の判断を自ら行うか、または、ステップＳ８１で、曲データベースから読み出した再生条件をアダプタ２６のCPU３２に供給し、CPU３２に、ステップＳ８４の判定処理を実行させる。

【０２２０】現在日時が再生終了日時を過ぎている場合、ステップＳ８５に進み、移動管理プログラム１３４は、コンテンツデータベース１１４に、選択されたコンテンツをHDD２１から消去させるとともに、曲データベースから、その選択されたコンテンツの情報を消去させる。ステップＳ８６において、移動管理プログラム１３４は、CPU３２に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ３４に保存させる。以後、処理は終了される。従って、この場合、コンテンツの移動が実行されない。

【０２２１】ステップＳ８４において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップＳ８７に進み、移動管理プログラム１３４は、その選択されたコンテンツの再生時課金条件（例えば、再生１回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、移動管理プログラム１３４は、ステップＳ８８において、PD用ドライバ１４３に、ポータブルデバイス６と通信させ、ポータブルデバイス６に課金機能が存在するか否かを判定する。ポータブルデバイス６に課金機能が存在しない場合には、選択されたコンテンツをポータブルデバイス６に転送する訳にはいかないので、ステップＳ８９において、移動管理プログラム１３４は、表示操作指示プログラム１１２に、例えば、「転送先が課金機能を有しておりません」のようなメッセージをディスプレイ２０に表示させ、コンテンツの移動処理を終了させる。

【０２２２】ステップＳ８７において再生時課金条件が登録されていないと判定された場合、または、ステップＳ８８において、ポータブルデバイス６に課金機能が存在すると判定された場合、ステップＳ９０に進み、移動

管理プログラム１３４は、選択されたコンテンツに関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップＳ９１に進み、移動管理プログラム１３４は、ポータブルデバイス６に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス６が、その再生条件を守る機能を有していない場合には、ステップＳ９２に進み、移動管理プログラム１３４は、表示操作指示プログラム１１２に、例えば、「転送先の装置が再生条件を守る機能を有しておりません」のようなメッセージをディスプレイ２０に表示させ、処理を終了させる。

【０２２３】ステップＳ９０において、再生条件が登録されていないと判定された場合、またはステップＳ９１において、ポータブルデバイス６が再生条件を守る機能を有していると判定された場合、再生条件等のチェック処理が終了され、図１２のステップＳ５６に戻る。

【０２２４】図１６は、ポータブルデバイス６が管理している（守ることが可能な）再生条件の例を表している。図１６に示す再生情報は、例えば、EEPROM６８に記憶されている。この例においては、アイテム１乃至アイテム３の各コンテンツについて、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム２についてのみ登録されており、アイテム１とアイテム３については登録されていない。従って、アイテム２のコンテンツが選択されたコンテンツとされた場合、再生回数の再生条件は守ることが可能であるが、アイテム１またはアイテム３のコンテンツが選択されたコンテンツとされた場合、再生回数の条件は守ることができないことになる。

【０２２５】次に、図１７のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するCPU１１による、図１２のステップＳ５８におけるフォーマット変換処理の詳細について説明する。ステップＳ１０１において、移動管理プログラム１３４は、コンテンツデータベース１１４に記録されている選択されたコンテンツのフォーマット（例えば、再生条件、使用条件、コピー条件などを含むヘッダなどの方式）を調べる。ステップＳ１０２において、移動管理プログラム１３４は、相手先の機器（今の場合、ポータブルデバイス６）に設定することが可能な条件を調べる。すなわち、移動管理プログラム１３４は、ポータブルデバイス６のCPU５３に設定可能な条件を問い合わせ、その回答を得る。ステップＳ１０３において移動管理プログラム１３４は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップＳ１０２で調べた条件に基づいて決定する。

【０２２６】ステップＳ１０４において、移動管理プログラム１３４は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップ

Ｓ１０５に進み、コンテンツをポータブルデバイス６に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス６が守ることができないので、そのようなポータブルデバイス６には、コンテンツを移動することが禁止されるのである。

【０２２７】ステップＳ１０４において設定可能な条件が存在すると判定された場合、ステップＳ１０６に進み、移動管理プログラム１３４は、利用条件変換プログラム１３９に、その条件を相手先の機能フォーマットの条件（例えば、ポータブルデバイス６に転送する際、ヘッダに格納される条件）に変換させる。そして、ステップＳ１０７において、移動管理プログラム１３４は、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス６は、設定された条件に従って（その条件を守って）、コンテンツを再生することが可能となる。

【０２２８】次に、図１８乃至図２０のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するCPU１１およびメインプログラムを実行するCPU５３による、HDD２１からポータブルデバイス６にコンテンツをコピーする場合の処理について説明する。この図１８乃至図２０のステップＳ１１１乃至ステップＳ１２７の処理は、コピー管理プログラム１３３により実行され、図１２乃至図１４のHDD２１からポータブルデバイス６へコンテンツを移動させる場合のステップＳ５１乃至ステップＳ６７の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択されたコンテンツの再生条件とのチェック処理が行われる。さらに、ポータブルデバイス６と、パーソナルコンピュータ１との間の相互認証処理の後、コンテンツが、パーソナルコンピュータ１のHDD２１からポータブルデバイス６のフラッシュメモリ６１に転送され、保存される。その後、ステップＳ１２８において、コピー管理プログラム１３３は、曲データベースのコピー回数カウンタを１だけインクリメントする。そして、ステップＳ１２９において、コピー管理プログラム１３３は、CPU３２に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ３４に保存させる。

【０２２９】次に、図２１のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するCPU１１およびメインプログラムを実行するCPU５３による、ポータブルデバイス６からHDD２１にコンテンツを移動する処理およびチェックインの処理について説明する。

【０２３０】始めに、コンテンツの移動の処理について説明する。ステップＳ１６１において、移動管理プログラム１３４は、ポータブルデバイス６のCPU５３に対してフラッシュメモリ６１に記憶されているコンテンツの情報の読み出しを要求する。CPU５３は、この要求に対応して、フラッシュメモリ６１に記憶されているコンテンツの情報をパーソナルコンピュータ１に送信する。移動管理プログラム１３４は、この情報に基づいて、ディスプレイ２０に、フラッシュメモリ６１に記憶されているコンテンツを選択するためのGUIを表示させる。使用者は、キーボード１８またはマウス１９を操作して、そのGUIに基づいて、ポータブルデバイス６からHDD２１（コンテンツデータベース１１４）に移動させるコンテンツを指定する。

【０２３１】ステップＳ１６２において、移動管理プログラム１３４は、認証プログラム１４１に、CPU５３との間において、相互認証処理を実行させ、通信用鍵を共有させる。この処理は、図１２のステップＳ５６における場合と同様の処理である。

【０２３２】次に、ステップＳ１６３において、CPU５３は、フラッシュメモリ６１に記憶されている暗号化されている選択されたコンテンツを読み出し、パーソナルコンピュータ１に転送する。移動管理プログラム１３４は、ステップＳ１６４において、ポータブルデバイス６から転送されてきたコンテンツを、１つのファイルとしてファイル名を付けて、コンテンツデータベース１１４（HDD２１）に保存する。この保存は、例えば、１つのファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

【０２３３】ステップＳ１６５において、CPU５３は、フラッシュメモリ６１に記憶されている選択されたコンテンツの暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ１に転送する。この暗号鍵は、例えば、図１４のステップＳ６７の処理でフラッシュメモリ６１に保存されていたものである。

【０２３４】ステップＳ１６６において、移動管理プログラム１３４は、ポータブルデバイス６から暗号鍵の転送を受けると、復号プログラム１４２に、それを通信用鍵で復号させ、暗号化プログラム１３７に、自分自身の保存用鍵で暗号化させる。ステップＳ１６７で、移動管理プログラム１３４は、コンテンツデータベース１１４に、ステップＳ１６４で保存したコンテンツのファイル名、そのコンテンツの情報、使用者がGUIを介して入力した曲名、ステップＳ１６６で暗号化した暗号鍵などを、HDD２１の曲データベースに登録させる。そして、ステップＳ１６８において、移動管理プログラム１３４は、利用条件管理プログラム１４０に、その曲データベース全体のハッシュ値をCPU３２に計算させ、不揮発性メモリ３４に保存させる。

【０２３５】ステップＳ１６９において、移動管理プログラム１３４は、ポータブルデバイス６に対して暗号鍵が保存されたことを通知し、そのコンテンツの削除を要求する。CPU５３は、パーソナルコンピュータ１から、そのコンテンツの削除が要求されてきたとき、ステップ

Ｓ１７０において、フラッシュメモリ６１に記憶されているそのコンテンツを削除する。

【０２３６】次に、ポータブルデバイス６からパーソナルコンピュータ１にコンテンツをチェックインする処理について説明する。ポータブルデバイス６からパーソナルコンピュータ１にコンテンツをチェックインする処理は、図２１のポータブルデバイス６からパーソナルコンピュータ１へコンテンツを移動させる場合と同様の処理である。すなわち、チェックインの処理は、パーソナルコンピュータ１においてチェックイン／チェックアウト管理プログラム１３２により実行され、図２１のステップＳ１６２乃至Ｓ１６６の処理が省略される。また、パーソナルコンピュータ１は、図２１のステップＳ１６７において、曲データベースに記録されている、チェックインされたコンテンツのチェックアウトできる回数を更新する処理を実行して、ステップＳ１７０の処理の後、コンテンツファイルの削除を確認することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

【０２３７】なお、ポータブルデバイス６のフラッシュメモリ６１がメモリカードとして着脱可能であるとき、パーソナルコンピュータ１は、チェックインの処理において、図２１のステップＳ１６２の相互認証の処理を実行する。

【０２３８】また、前述のように、所定のパーソナルコンピュータからチェックアウトされたコンテンツが、該パーソナルコンピュータにのみチェックインできるようになっており、チェックイン処理の前処理として、選択されたコンテンツが、チェックインを行うＰＣからチェックアウトされたかを判断し、該ＰＣからチェックアウトされたものではないと判断されたらば、チェックインを行わないように処理するステップが存在する。例えば、図５のフィールド２１３の×がついたコンテンツをチェックインしようとした場合がそれにあたる。

【０２３９】次に、コンテンツ管理プログラム１１１を実行するCPU１１およびメインプログラムを実行するCPU５３による、ポータブルデバイス６からHDD２１へコンテンツをコピーする場合の処理について、図２２のフローチャートを参照して説明する。この図２２に示すステップＳ１８１乃至ステップＳ１８８の処理は、図２１のポータブルデバイス６からHDD２１へコンテンツを移動させる場合の処理におけるステップＳ１６１乃至ステップＳ１６８の処理と同様の処理である。すなわち、コピー処理の場合は、コピー管理プログラム１３３により実行され、図２１のステップＳ１６９，Ｓ１７０の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

【０２４０】次に、図２３のフローチャートを参照して、EMDサーバ４およびコンテンツ管理プログラム１１１を実行するCPU１１による、EMDサーバ４から転送を受けたコンテンツをHDD２１にコピーする処理について説明する。

ステップＳ２０１において、購入用プログラム１４４は、図５に示すボタン２０２がクリックされて、使用者からEMDサーバ４へのアクセスが指令されたとき、通信部２５を制御し、ネットワーク２を介してEMDサーバ４にアクセスさせる。EMDサーバ４は、このアクセスに対応して、自分自身が保持しているコンテンツの曲番号、曲名、各情報などの情報を、ネットワーク２を介してパーソナルコンピュータ１に転送する。購入用プログラム１４４は、通信部２５を介して、この情報を取得したとき、表示操作指示プログラム１１２に、それをインタフェース１７を介してディスプレイ２０に表示させる。使用者は、ディスプレイ２０に表示されたGUIを利用して、ステップＳ２０２において、コピーを希望するコンテンツを指定する。この指定情報は、ネットワーク２を介してEMDサーバ４に転送される。ステップＳ２０３において、購入用プログラム１４４は、EMDサーバ４との間において、ネットワーク２を介して相互認証処理を実行し、通信用鍵を共有する。

【０２４１】パーソナルコンピュータ１とEMDサーバ４との間で行われる相互認証処理は、例えば、ISO　９７９８－３で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ１は、自分自身の秘密鍵とEMDサーバ４の公開鍵を予め有しており、EMDサーバ４は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ１の公開鍵は、EMDサーバ４から転送したり、あるいはパーソナルコンピュータ１に予め配布されている証明書（certificate）をパーソナルコンピュータ１からEMDサーバ４に転送し、その証明書をEMDサーバ４が確認し、公開鍵を得るようにしてもよい。さらに、ステップＳ２０４において、購入用プログラム１４４は、EMDサーバ４との間において課金に関する処理を実行する。この課金の処理の詳細は、図２４のフローチャートを参照して後述する。

【０２４２】次に、ステップＳ２０５において、EMDサーバ４は、パーソナルコンピュータ１に対して、ステップＳ２０２で指定された、暗号化されているコンテンツをネットワーク２を介してパーソナルコンピュータ１に転送する。このとき、時刻情報も適宜転送される。ステップＳ２０６において、購入用プログラム１４４は、コンテンツデータベース１１４に、転送を受けたコンテンツにファイル名を付けてHDD２１に１つのコンテンツファイル１６１として保存させる。ステップＳ２０７において、EMDサーバ４は、さらに、そのコンテンツの暗号鍵をステップＳ２０３でパーソナルコンピュータ１と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ１へ転送する。

【０２４３】購入用プログラム１４４は、ステップＳ２０８において、復号プログラム１４２に、EMDサーバ４

より転送を受けた暗号鍵を単独で、またはアダプタ２６のCPU３２と共同して通信用鍵を用いて復号させ、暗号化プログラム１３７に、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化させる。ステップＳ２０９において、購入用プログラム１４４は、コンテンツデータベース１１４に、そのコンテンツのファイル名、コンテンツの情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、HDD２１の曲データベースに登録させる。さらに、ステップＳ２１０において、購入用プログラム１４４は、その曲データベース全体のハッシュ値をCPU３２に計算させ、不揮発性メモリ３４に保存させる。

【０２４４】なお、ステップＳ２０５においてEMDサーバ４は、コンテンツとともに、時刻データをパーソナルコンピュータ１に送信する。この時刻データは、パーソナルコンピュータ１からアダプタ２６に転送される。アダプタ２６のCPU３２は、パーソナルコンピュータ１より転送されてきた時刻データを受信すると、ステップＳ２１１において、RTC３５の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ２６のRTC３５の時刻情報を修正するようにしたので、アダプタ２６を常に正しい時刻情報を保持することが可能となる。

【０２４５】次に、図２４のフローチャートを参照して、EMDサーバ４およびコンテンツ管理プログラム１１１を実行するCPU１１による、図２３のステップＳ２０４における課金に関する処理の詳細について説明する。ステップＳ２２１において、購入用プログラム１４４は、ステップＳ２０１でEMDサーバ４から伝送されてきた価格情報の中から、ステップＳ２０２で指定された選択されたコンテンツの価格情報を読み取り、これをHDD２１上の課金ログに書き込む。図２５は、このような課金ログの例を表している。この例においては、使用者は、アイテム１乃至アイテム３を、EMDサーバ４からコピーしており、アイテム１とアイテム２の領域は５０円とされ、アイテム３の料金は６０円とされている。その時点における課金ログのハッシュ値も、CPU３２により計算され、不揮発性メモリ3.4に登録されている。

【０２４６】次に、ステップＳ２２２において、購入用プログラム１４４は、ステップＳ２２１で書き込んだ課金ログをHDD２１から読み出し、これをネットワーク２を介してEMDサーバ４に転送する。EMDサーバ４は、ステップＳ２２３において、パーソナルコンピュータ１から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMDサーバ４は、内蔵するデータベースに、パーソナルコンピュータ１の使用者から伝送されてきた課金ログを追加更新する。そして、ステップＳ２２４において、EMDサーバ４は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップＳ２２５に進み、EMDサーバ４は、決裁に必要な商品名、金額などを決裁サーバ（図示せず）に転送する。そして、ステップＳ２２６において、決裁サーバは、パーソナルコンピュータ１の使用者に対する決裁処理を実行する。ステップＳ２２４において、決裁は直ちには行われないと判定された場合、ステップＳ２２５とＳ２２６の処理はスキップされる。すなわち、この処理は、例えば、月に１回など、定期的にその後実行される。

【０２４７】次に、図２６と図２７のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するCPU１１による、音声入出力インタフェース２４のIEC60958端子２４ａから入力された、図示せぬCDプレーヤなどからの再生されたコンテンツを、HDD２１にコピーする場合の処理について説明する。ステップＳ２４１において、使用者は、CDプレーヤのIEC60958出力端子を、パーソナルコンピュータ１の音声入出力インタフェース２４のIEC60958端子２４ａに接続する。ステップＳ２４２において、使用者は、キーボード１８またはマウス１９を操作し、CDプレーヤからコピーするコンテンツの曲名（または、コンテンツに対応する番号）を入力する。そして、ステップＳ２４３において使用者は、CDプレーヤのボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ１との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ１のキーボード１８またはマウス１９を介して再生開始指令を入力することで、CDプレーヤにCDの再生を開始させることも可能である。

【０２４８】CDプレーヤにおいて、CDの再生が開始されると、ステップＳ２４４において、CDプレーヤから出力されたコンテンツが、IEC60958端子２４ａを介してパーソナルコンピュータ１に転送されてくる。ステップＳ２４５において、コピー管理プログラム１３３は、IEC60958端子２４ａを介して入力されてくるデータから、SCMS（Serial Copy Management System）データを読み取る。このSCMSデータには、コピー禁止、コピー１回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップＳ２４６において、CPU１１は、SCMSデータがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップＳ２４７に進み、コピー管理プログラム１３３は、表示操作指示プログラム１１２に、例えば、「コピーが禁止されています」といったメッセージをディスプレイ２０に表示させ、コピー処理を終了する。すなわち、この場合には、HDD２１へのコピーが禁止される。

【０２４９】コピー管理プログラム１３３は、ステップＳ２４６において、ステップＳ２４５で読み取ったSCMS情報がコピー禁止を表していないと判定した場合、ステップＳ２４８に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップＳ２４９において判定する。ウォータマー

クコードがコピー禁止を表している場合には、ステップＳ２４７に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

【０２５０】ステップＳ２４９において、ウォータマークがコピー禁止を表していないと判定された場合、ステップＳ２５０に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択されたコンテンツが既に登録されていれば、ステップＳ２５１，Ｓ２５２の処理で、処理が終了される。この処理は、図７のステップＳ１３，Ｓ１４の処理と同様の処理である。

【０２５１】選択されたコンテンツがまだHDD２１に登録されていないコンテンツであれば、ステップＳ２５３乃至Ｓ２５８で、その登録処理が実行される。このステップＳ２５３乃至ステップＳ２５８の処理は、ステップＳ２５７において、IEC60958端子２４ａから供給されてくるSCMS情報も曲データベースに登録される点を除き、図７のステップＳ１９乃至ステップＳ２４の処理と同様の処理であるので、その説明は省略する。

【０２５２】次に、図２８と図２９のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するCPU１１による、コンテンツをHDD２１からIEC60958端子２４ａに出力（再生）する場合の処理について説明する。ステップＳ２７１乃至ステップＳ２７３において、図１８のステップＳ１１１乃至Ｓ１１３における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップＳ２７４に進み、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、HDD２１の曲データベースにアクセスさせ、そこに登録されている曲の情報を読み出させ、ディスプレイ２０に表示させる。使用者は、その表示を見て、キーボード１８またはマウス１９を適宜操作して、再生出力するコンテンツを選択する。ステップＳ２７５において、表示操作指示プログラム１１２は、選択されたコンテンツの再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図３０のフローチャートを参照して後述する。

【０２５３】次に、ステップＳ２７６において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、ステップＳ２７４において選択されたコンテンツの暗号鍵を曲データベースから読み出させ、復号プログラム１４２に保存用鍵で復号させる。ステップＳ２７７において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、選択されたコンテンツのSCMS情報を曲データベースから読み出させ、IEC60958端子２４ａから出力する

SCMS情報を、SCMSシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は１だけインクリメントされ、新たなSCMS情報とされる。ステップＳ２７８において、表示操作指示プログラム１１２はさらに、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、選択されたコンテンツのISRCを曲データベースから読み出させる。

【０２５４】次に、ステップＳ２７９において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、曲データベースから選択されたコンテンツファイル名を読み出させ、そのファイル名を基に、そのコンテンツをHDD２１から読み出させる。表示操作指示プログラム１１２はさらに、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、そのコンテンツに対応する暗号鍵を曲データベースから読み出させ、復号プログラム１４２に、保存用鍵で復号させ、復号した暗号鍵を用いて、暗号化されているコンテンツを復号する。圧縮／伸張プログラム１３８は、さらに、そのコンテンツの圧縮符号を復号（伸張）する。ステップＳ２８０において、表示操作指示プログラム１１２は、ドライバ１１７に、ステップＳ２７９で、復号したデジタルデータであるコンテンツを、ステップＳ２７７で決定したSCMS情報、並びにステップＳ２７８で読み出したISRC情報とともに、IEC60958の規定に従って、IEC60958端子２４ａから出力させる。さらにまた、表示操作指示プログラム１１２は、例えば、図示せぬリアルプレーヤ（商標）などのプログラムを動作させ、デジタルデータであるコンテンツをアナログ化させ、音声入出力インタフェース２４のアナログ出力端子から出力させる。

【０２５５】ステップＳ２８１において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、曲データベース中の再生回数カウンタの値を１だけインクリメントさせる。そして、ステップＳ２８２において、選択されたコンテンツに再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップＳ２８３に進み、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、対応する料金を課金ログに書き込ませ、ステップＳ２８４において、表示操作指示プログラム１１２は、利用条件管理プログラム１４０に、曲データベース全体のハッシュ値をCPU３２に計算させ、不揮発性メモリ３４に記憶させる。ステップＳ２８２において、選択されたコンテンツに再生時課金条件が付加されていないと判定された場合、ステップＳ２８３とステップＳ２８４の処理はスキップされる。

【０２５６】次に、図３０のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するCPU１１による、図２８のステップＳ２７５の再生条件等のチ

ェック処理の詳細について説明する。ステップＳ３０１において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、曲データベースの各種条件を読み出させる。ステップＳ３０２において利用条件管理プログラム１４０は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップＳ３０３に進み、コンテンツ管理プログラム１１１を介して、コンテンツデータベース１１４に、選択されたコンテンツをHDD２１から削除させるとともに、曲データベースから選択されたコンテンツの情報を削除させる。ステップＳ３０４において、表示操作指示プログラム１１２はさらに、利用条件管理プログラム１４０に、曲データベースの新たなハッシュ値をCPU３２に計算させ、そのハッシュ値を不揮発性メモリ３４に保存させる。この場合、再生出力は禁止される。

【０２５７】ステップＳ３０２において、再生回数が制限回数を過ぎていないと判定された場合、ステップＳ３０５に進み、利用条件管理プログラム１４０２は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した場合と同様にステップＳ３０３において、選択されたコンテンツをHDD２１から削除させるとともに、曲データベースからも削除させる。そして、ステップＳ３０４において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

【０２５８】ステップＳ３０５において、再生終了日時が現在日時を過ぎていないと判定された場合は、ステップＳ３０６に進み、CPU３２は、その選択されたコンテンツに対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップＳ３０７に進み、表示操作指示プログラム１１２は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ２０に表示させる。ステップＳ３０６において、再生時課金条件が付加されていないと判定された場合、ステップＳ３０７の処理はスキップされる。

【０２５９】次に、図３１と図３２のフローチャートを参照して、コンテンツ管理プログラム１１１を実行するCPU１１およびメインプログラムを実行するCPU５３による、HDD２１からポータブルデバイス６経由でコンテンツを出力（再生）する場合の処理について説明する。ステップＳ３２１乃至ステップＳ３２５において、曲データベースの改竄チェックと選択されたコンテンツの指定、並びに選択されたコンテンツの再生条件等のチェック処理が行われる。その処理は、図２８のステップＳ２７１乃至ステップＳ２７５の処理と同様の処理であるので、その説明は省略する。

【０２６０】ステップＳ３２６において、ポータブルデバイス６とパーソナルコンピュータ１の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップＳ３２７において、表示操作指示プログラム１１２は、ポータブルデバイス６に対して、これから送る暗号化されているコンテンツを再生するように命令する。ステップＳ３２８において、表示操作指示プログラム１１２は、ステップＳ３２４で、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４に、指定された選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツをHDD２１から読み出させる。表示操作指示プログラム１１２は、ステップＳ３２９において、コンテンツ管理プログラム１１１に、コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイス６の方式のものに変換する処理を実行させる。そして、ステップＳ３３０において、表示操作指示プログラム１１２は、暗号化プログラム１３７に、ステップＳ３２９において変換したコンテンツを通信用鍵で暗号化させ、ポータブルデバイス６に転送する。

【０２６１】ステップＳ３３１において、ポータブルデバイス６のCPU５３は、ステップＳ３２７において、パーソナルコンピュータ１から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップＳ３３２において、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４に、曲データベースの再生回数カウントを１だけインクリメントさせる。さらに、ステップＳ３３３において、表示操作指示プログラム１１２は、選択されたコンテンツに再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップＳ３３４において、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４に、その料金を課金ログに書き込ませ、ステップＳ３３５において、CPU３２に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択されたコンテンツに再生時課金条件が付加されていない場合には、ステップＳ３３４，ステップＳ３３５の処理はスキップされる。

【０２６２】本発明においては、コンテンツが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU１１を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

【０２６３】さらに、上述したように、CPU１１の機能の一部は、ハードウェアとしてのアダプタ２６に分担され、両者が共働して各種の処理を実行するようになされている。これにより、より安全性を高めることが可能となっている。

【０２６４】例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるので

はなく、アダプタ２６の不揮発性メモリ３４に保存される。すなわち、図８のステップＳ３２，Ｓ３３などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ３４に記憶されているものとされる。これにより、例えば、他の記録媒体にコピーまたは移動させる前に、HDD２１に保存されているコンテンツを含む記録内容の全てをバックアップしておき、HDD２１から、そこに保存されているコンテンツを他の記録媒体にコピーまたは移動した後、HDD２１にバックアップしておいた記録内容に含まれるコンテンツを再びリストアするようにすることで、利用条件を無視して、実質的に際限なく、コピーまたは移動ができてしまうようなことが防止される。

【０２６５】例えば、図３３に示すように、HDD２１にコンテンツＡ，Ｂが保存されている場合、不揮発性メモリ３４には、コンテンツＡとコンテンツＢの情報に対応するハッシュ値が保存されている。この状態において、HDD２１のコンテンツＡ，Ｂを含む記録データの一部または全部を他の記録媒体２７１にバックアップしたとする。その後、HDD２１に保存されているコンテンツＡとコンテンツＢのうち、コンテンツＡを他の記録媒体２７２に移動させた場合、その時点において、HDD２１に記録されているコンテンツは、コンテンツＢだけとなるので、不揮発性メモリ３４のハッシュ値も、コンテンツＢに対応するハッシュ値に変更される。

【０２６６】従って、その後、記録媒体２７１にバックアップしておいたHDD２１のコンテンツＡ，Ｂを含む記録データの一部または全部をHDD２１にリストアして、HDD２１に、再びコンテンツＡとコンテンツＢを保存させたとしても、不揮発性メモリ３４には、コンテンツＢの情報から演算されたハッシュ値が記憶されており、コンテンツＡとコンテンツＢの情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、HDD２１に記憶されているコンテンツＡとコンテンツＢに基づくハッシュ値が、不揮発性メモリ３４に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、HDD２１に保存されているコンテンツＡとコンテンツＢの利用が制限されてしまうことになる。

【０２６７】さらに、上述したように、アダプタ２６は、RTC３５を内蔵しており、このRTC３５の値は、正しい認証結果が得られた他の装置（例えば、EMDサーバ４）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ１が管理するものではなく、RTC３５が出力するものが利用される。従って、使用者が、パーソナルコンピュータ１の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

【０２６８】また、アダプタ２６は、暗号化されて転送されてきたプログラムをROM３６に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図３４のフローチャートを参照して説明する。

【０２６９】すなわち、パーソナルコンピュータ１は、アダプタ２６に対して、所定の処理を実行させたいとき、ステップＳ３５１において、アダプタ２６に実行させるべきプログラムをRAM１３に予め記憶されている暗号鍵を用いて暗号化してアダプタ２６に転送する。アダプタ２６のROM３６には、パーソナルコンピュータ１から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。CPU３２は、このROM３６に記憶されているプログラムに従って、パーソナルコンピュータ１から転送されてきた暗号化されているプログラムをステップＳ３５２において復号する。そして、ステップＳ３１３において、CPU３２は、復号したプログラムをRAM３３に展開し、ステップＳ３５４において、そのプログラムを実行する。

【０２７０】例えば、上述したように、パーソナルコンピュータ１のCPU１１は、HDD２１の曲データベースのハッシュ値をアダプタ２６に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ２６のCPU３２に転送する。CPU３２は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ３４に記憶させる。あるいは、そのハッシュ値を、CPU３２は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ１のCPU１１に転送する。

【０２７１】図３５は、アダプタ２６の内部のより具体的な構成を表している。アダプタ２６は、半導体ICとして形成される。アダプタ２６は、図２に示したインタフェース３１、CPU３２、RAM３３、不揮発性メモリ３４、RTC３５、ROM３６以外に、RAM３３に対する書き込みと読み出しを制御するRAMコントローラ３０１、並びに論理回路３０２を有している。論理回路３０２は、例えば、暗号化されているコンテンツを解読した後、解読したデータをアダプタ２６から直接出力するような場合の処理のために用いられる。

【０２７２】これらのインタフェース３１乃至ROM３６、RAMコントローラ３０１、並びに論理回路３０２は、半導体IC内に一体的に組み込まれ、外部からは分解できないように構成されている。

【０２７３】水晶振動子３１１は、アダプタ２６が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路３１２は、RTC３５を動作させるための発振回路である。バッテリ３１３は、発振回路３１２、不揮発性メモリ３４、およびRTC３５に対してバックアップ用の電力を供給している。アダプタ２６のその他の回路には、パーソナルコンピュータ１

の電源供給回路３２１からの電力が供給されている。

【０２７４】不揮発性メモリ３４は、書き込み消去可能なROMで構成することも可能であるが、バッテリ３１３からのバックアップ電源でバックアップされるRAMで構成する場合には、例えば、図３６に示すように、不揮発性メモリ３４の上に保護アルミニウム層３５１を形成し、さらに、その保護アルミニウム層３５１と同一平面上となるように、不揮発性メモリ３４にバッテリ３１３からの電力を供給する電源パターン３５２を形成するようにすることができる。このようにすると、例えば、不揮発性メモリ３４を改竄すべく、保護アルミニウム層３５１を削除しようとすると、同一平面上の電源パターン３５２も削除されてしまい、不揮発性メモリ３４に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

【０２７５】さらに、図３７に示すように、不揮発性メモリ３４に対するデータの書き込みまたは読み出しのための配線４０１－１乃至４０１－３は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線４０１－３からデータを読み出すためには、上方の配線４０１－１，４０１－２を除去しなければならず、複数の配線４０１－１，４０１－２，４０１－３から同時にデータを読み取ることができなくなる。

【０２７６】さらにまた、不揮発性メモリ３４は、配線４０１－１乃至４０１－３を冗長に形成するようにすることができる。例えば、不揮発性メモリ３４内部に形成される配線４０１－１乃至４０１－３が不揮発性メモリ３４を構成するトランジスタなどの素子を結合するとき、その経路は、例え、直線的に結合が可能であっても、直線的には形成されず、所定の長さとなるように形成される。このようにすることで、配線４０１－１乃至４０１－３の長さは、本来必要な長さ以上の長さとなり、配線に必要な最短の長さの場合に比較して大きな寄生容量を有することとなる。

【０２７７】不揮発性メモリ３４からデータを読み出すために設計されている専用の回路（半導体ICとしてのアダプタ２６に内蔵されている）は、その寄生容量にマッチングしたインピーダンスを設定することで、不揮発性メモリ３４が記憶しているデータを正常に読み出すことができる。しかしながら、不揮発性メモリ３４に記憶されているデータを読み出すべく、プローブを配線４０１－１乃至４０１－３に接続させると、その寄生容量とプローブによる合成の容量が影響して、データを正常に読み出すことが困難になる。

【０２７８】次に、ポータブルデバイス６がパーソナルコンピュータ１から所定のデータを受け取る場合の、相互認証の処理を図３８および図３９のフローチャートを参照して説明する。ステップＳ４０１において、パーソナルコンピュータ１のCPU１１は、乱数Ｎａを生成する。ステップＳ４０２において、パーソナルコンピュータ１のCPU１１は、インターフェース１７に、パーソナルコンピュータ１のID、鍵のカテゴリ番号Ｇ、および乱数Ｎａをポータブルデバイス６へ送信させる。

【０２７９】ステップＳ４２１において、ポータブルデバイス６のCPU５３は、乱数Ｎｂを生成する。ステップＳ４２２において、ポータブルデバイス６は、USBコントローラ５７を介して、パーソナルコンピュータ１から送信されたパーソナルコンピュータ１のID、鍵のカテゴリ番号Ｇ、および乱数Ｎａを受信する。ステップＳ４２３において、ポータブルデバイス６のCPU５３は、鍵のカテゴリ番号Ｇから、マスター鍵K_{M_n}の鍵番号ｊを求める。

【０２８０】ステップＳ４２４において、ポータブルデバイス６のCPU５３は、ｊ番目のマスター鍵$K_{M_n(j)}$を求める。ステップＳ４２５において、ポータブルデバイス６のCPU５３は、パーソナルコンピュータ１のIDに、マスター鍵$K_{M_n(j)}$を基にしたＳＨＡなどのハッシュ関数を適用し、鍵K_{n_b}を求める。

【０２８１】ステップＳ４２６において、ポータブルデバイス６のCPU５３は、乱数Ｎａ、乱数Ｎｂ、およびパーソナルコンピュータ１のIDに、鍵K_{n_b}を基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ１を求める。ステップＳ４２７において、ポータブルデバイス６のCPU５３は、乱数Ｓｂを生成する。

【０２８２】ステップＳ４２８において、ポータブルデバイス６のCPU５３は、USBコントローラ５７に、乱数Ｎａ、乱数Ｎｂ、鍵番号ｊ、および乱数Ｓｂをパーソナルコンピュータ１へ送信させる。

【０２８３】ステップＳ４０３において、パーソナルコンピュータ１は、インターフェース１７を介して、乱数Ｎａ、乱数Ｎｂ、鍵番号ｊ、および乱数Ｓｂを受信する。ステップＳ４０４において、パーソナルコンピュータ１のCPU１１は、鍵番号ｊを基に、個別鍵K_{I_n}に含まれる鍵K_{n_b}を求める。ステップＳ４０５において、パーソナルコンピュータ１のCPU１１は、乱数Ｎａ、乱数Ｎｂ、およびパーソナルコンピュータ１のIDに、鍵K_{n_b}を基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ２を求める。

【０２８４】ステップＳ４０６において、パーソナルコンピュータ１のCPU１１は、受信した乱数Ｒ１と、ステップＳ４０５で生成した乱数Ｒ２とが等しいか否かを判定し、乱数Ｒ１と乱数Ｒ２とが等しくないと判定された場合、正当なポータブルデバイスではないので、ポータブルデバイス６を認証せず、処理は終了する。ステップＳ４０６において、乱数Ｒ１と乱数Ｒ２とが等しいと判定された場合、ポータブルデバイス６は正当なポータブルデバイスなので、ステップＳ４０７に進み、パーソナルコンピュータ１のCPU１１は、乱数Ｓａを生成する。

【０２８５】ステップＳ４０８において、パーソナルコンピュータ１のCPU１１は、乱数Ｎｂおよび乱数Ｎａに、鍵K_{ab}を基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ３を求める。ステップＳ４０９において、パーソナルコンピュータ１のCPU１１は、インターフェース１７に、乱数Ｒ３および乱数Ｓｂをポータブルデバイス６へ送信させる。ステップＳ４１０において、パーソナルコンピュータ１のCPU１１は、乱数Ｓａおよび乱数Ｓｂに、鍵K_{ab}を基にしたＳＨＡなどのハッシュ関数を適用し、一時鍵K_sを求める。

【０２８６】ステップＳ４２９において、ポータブルデバイス６のCPU５３は、USBコントローラ５７を介して、乱数Ｒ３および乱数Ｓｂを受信する。ステップＳ４３０において、ポータブルデバイス６のCPU５３は、乱数Ｎｂおよび乱数Ｎａに、鍵K_{ab}を基にしたＳＨＡなどのハッシュ関数を適用し、乱数Ｒ４を求める。ステップＳ４３１において、ポータブルデバイス６のCPU５３は、受信した乱数Ｒ３と、ステップＳ４３０で生成した乱数Ｒ４とが等しいか否かを判定し、乱数Ｒ３と乱数Ｒ４とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ１を認証せず、処理は終了する。ステップＳ４３１において、乱数Ｒ３と乱数Ｒ４とが等しいと判定された場合、パーソナルコンピュータ１は正当なパーソナルコンピュータなので、ステップＳ４３２に進み、ポータブルデバイス６のCPU５３は、乱数Ｓａおよび乱数Ｓｂに、鍵K_{ab}を基にしたＳＨＡなどのハッシュ関数を適用し、一時鍵K_sを求める。

【０２８７】以上のように、パーソナルコンピュータ１およびポータブルデバイス６は、相互認証し、共通の一時鍵K_sを得る。なお、ステップＳ４２５、ステップＳ４２６、ステップＳ４０５、ステップＳ４０８、ステップＳ４１０、ステップＳ４３０、およびステップＳ４３２において、ＳＨＡなどのハッシュ関数を適用するとして説明したが、ＤＥＳなどを適用しても良い。

【０２８８】次に、パーソナルコンピュータ１がポータブルデバイス６に所定のデータを送信する場合の、相互認証の処理を図４０および図４１のフローチャートを参照して説明する。ステップＳ４５１において、パーソナルコンピュータ１のCPU１１は、乱数Ｎａを生成する。ステップＳ４５２において、パーソナルコンピュータ１は、インターフェース１７を介して、パーソナルコンピュータ１のID、パーソナルコンピュータ１の鍵のカテゴリ番号Ｇｐ、ポータブルデバイス６の鍵のカテゴリ番号Ｇｓ、および乱数Ｎａをポータブルデバイス６に送信する。

【０２８９】ステップＳ４８１において、ポータブルデバイス６のCPU５３は、乱数Ｎｂを生成する。ステップＳ４８２において、ポータブルデバイス６は、USBコントローラ５７を介して、パーソナルコンピュータ１から送信されたパーソナルコンピュータ１のID、パーソナルコンピュータ１の鍵のカテゴリ番号Ｇｐ、ポータブルデバイス６の鍵のカテゴリ番号Ｇｓ、および乱数Ｎａを受信する。ステップＳ４８３において、ポータブルデバイス６のCPU５３は、ポータブルデバイス６の鍵のカテゴリ番号Ｇｓから、マスター鍵K_{ms}の鍵番号ｊを求める。

【０２９０】ステップＳ４８４において、ポータブルデバイス６のCPU５３は、ｊ番目のマスター鍵$K_{ms[j]}$を求める。ステップＳ４８５において、ポータブルデバイス６のCPU５３は、パーソナルコンピュータ１のIDに、マスター鍵$K_{ms[j]}$を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵K_{ab}を求める。ステップＳ４８６において、ポータブルデバイス６のCPU５３は、パーソナルコンピュータ１の鍵のカテゴリ番号Ｇｐを基に、マスター鍵K_{ms}の鍵番号ｋを求める。ステップＳ４８７において、ポータブルデバイス６のCPU５３は、鍵K_{ab}に、マスター鍵$K_{ms[k]}$を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵K'_{ab}を求める。

【０２９１】ステップＳ４８８において、ポータブルデバイス６のCPU５３は、乱数Ｎａおよび乱数Ｎｂに、鍵K'_{ab}を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ１を求める。ステップＳ４８９において、ポータブルデバイス６のCPU５３は、乱数Ｓｂを生成する。

【０２９２】ステップＳ４９０において、ポータブルデバイス６のCPU５３は、USBコントローラ５７に、ポータブルデバイス６のID、乱数Ｎｂ、乱数Ｒ１、鍵番号ｊ、および乱数Ｓｂをパーソナルコンピュータ１へ送信させる。

【０２９３】ステップＳ４５３において、パーソナルコンピュータ１は、インターフェース１７を介して、ポータブルデバイス６のID、乱数Ｎｂ、乱数Ｒ１、鍵番号ｊ、および乱数Ｓｂを受信する。ステップＳ４５４において、パーソナルコンピュータ１のCPU１１は、ポータブルデバイス６のIDに、パーソナルコンピュータ１のマスター鍵K_{MP}を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、マスター鍵K_mを求める。ステップＳ４５５において、パーソナルコンピュータ１のCPU１１は、ｊ番目の個別鍵K_{js}を求める。ステップＳ４５６において、パーソナルコンピュータ１のCPU１１は、乱数Ｎａおよび乱数Ｎｂに、鍵K_{js}を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、鍵K'_{ab}を求める。ステップＳ４５７において、パーソナルコンピュータ１のCPU１１は、乱数Ｎａおよび乱数Ｎｂに、鍵K'_{ab}を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ２を求める。

【０２９４】ステップＳ４５８において、パーソナルコンピュータ１のCPU１１は、受信した乱数Ｒ１と、ステップＳ４５７で生成した乱数Ｒ２とが等しいか否かを判

定し、乱数Ｒ１と乱数Ｒ２とが等しくないと判定された場合、正当なポータブルデバイスではないので、ポータブルデバイス６を認証せず、処理は終了する。ステップＳ４５８において、乱数Ｒ１と乱数Ｒ２とが等しいと判定された場合、ポータブルデバイス６は正当なポータブルデバイスなので、ステップＳ４５９に進み、パーソナルコンピュータ１のCPU１１は、乱数Ｓａを生成する。

【０２９５】ステップＳ４６０において、パーソナルコンピュータ１のCPU１１は、乱数Ｎｂおよび乱数Ｎａに、鍵K_{ab}を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ３を求める。ステップＳ４６１において、パーソナルコンピュータ１のCPU１１は、インターフェース１７を介して、ポータブルデバイス６に、乱数Ｒ３および乱数Ｓｂを送信する。ステップＳ４６２において、パーソナルコンピュータ１のCPU１１は、乱数Ｓａおよび乱数Ｓｂに、鍵K'_{ab}を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、一時鍵K_sを求める。

【０２９６】ステップＳ４９１において、ポータブルデバイス６のCPU５３は、USBコントローラ５７を介して、乱数Ｒ３および乱数Ｓｂを受信する。ステップＳ４９２において、ポータブルデバイス６のCPU５３は、乱数Ｎｂおよび乱数Ｎａに、鍵K_{ab}を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、乱数Ｒ４を求める。ステップＳ４９３において、ポータブルデバイス６のCPU５３は、受信した乱数Ｒ３と、ステップＳ４９２で生成した乱数Ｒ４とが等しいか否かを判定し、乱数Ｒ３と乱数Ｒ４とが等しくないと判定された場合、正当なパーソナルコンピュータではないので、パーソナルコンピュータ１を認証せず、処理は終了する。ステップＳ４９３において、乱数Ｒ３と乱数Ｒ４とが等しいと判定された場合、パーソナルコンピュータ１は、正当なパーソナルコンピュータなので、ステップＳ４９４に進み、ポータブルデバイス６のCPU５３は、乱数Ｓａおよび乱数Ｓｂに、鍵K_{ab}を基にしたＳＨＡなどのハッシュ関数を適用ハッシュ関数を適用し、一時鍵K_sを求める。

【０２９７】このように、パーソナルコンピュータ１およびポータブルデバイス６は、相互認証し、共通の一時鍵K_sを得る。図４０および図４１のフローチャートに示した手続きは、図３８および図３９のフローチャートに示す手続きよりも、いわゆる”なりすまし”に対する防御（検出）が強力である。なお、ステップＳ４８５、ステップＳ４８７、ステップＳ４８８、ステップＳ４５４、ステップＳ４５６、ステップＳ４５７、ステップＳ４６０、ステップＳ４６２、ステップＳ４９２、およびステップＳ４９４において、ＳＨＡなどのハッシュ関数を適用するとして説明したが、ＤＥＳなどを適用しても良い。

【０２９８】以上のように、パーソナルコンピュータ１およびポータブルデバイス６は、相互認証の後に行われる処理に対応し、検出力が異なる相互認証の手続きを使い分けることにより、効率的かつ強力に、なりすましによる攻撃に対応することができる。

【０２９９】次に、ソースプログラムを暗号化する処理を、図４２のフローチャートを参照して説明する。ステップＳ５０１において、パーソナルコンピュータ１は、インターネット接続インターフェース１１を介して、図示せぬ認証局に署名を付したソースプログラムを送信する。ステップＳ５０２において、認証局は、署名を基に、受信したソースプログラムに改竄が発見されたか否かを判定し、受信したソースプログラムに改竄が発見された場合、処理は継続できないので、処理は終了する。

【０３００】ステップＳ５０２において、受信したソースプログラムに改竄が発見さなかった場合、ステップＳ５０３に進み、認証局は、受信したソースプログラムを認証局の秘密鍵で暗号化する。ステップＳ５０４において、認証局は、暗号化したソースプログラムをパーソナルコンピュータ１に送信する。ステップＳ５０５において、パーソナルコンピュータ１は、受信したソースプログラムを、HDD２１に記録し、処理は終了する。

【０３０１】以上のように、ソースプログラムは、暗号化される。なお、認証局に代わり、EMDサーバ４または所定の安全なサーバが、ソースプログラムを暗号化するようにしてもよい。

【０３０２】次に、暗号化されたソースプログラムをアダプタ２６が実行する処理を、図４３のフローチャートを参照して説明する。ステップＳ５２１において、アダプタ２６のCPU３２は、パーソナルコンピュータ１から受信した、暗号化されたソースプログラムを、不揮発性メモリ３４に予め記憶されている認証局の公開鍵で復号する。ステップＳ５２２において、アダプタ２６のCPU３２は、インタープリタを起動し、復号されたソースプログラムを実行する。

【０３０３】ステップＳ５２３において、アダプタ２６のCPU３２は、ソースプログラムを実行して得られた結果を、パーソナルコンピュータ１に送信するか否かを判定し、結果をパーソナルコンピュータ１に送信しないと判定された場合、処理は終了する。ステップＳ５２３において、結果をパーソナルコンピュータ１に送信すると判定された場合、ステップＳ５２４に進み、アダプタ２６のCPU３２は、ソースプログラムを実行して得られた結果を所定の鍵で暗号化する。ステップＳ５２５において、アダプタ２６のCPU３２は、インターフェース３１を介して、暗号化された結果をパーソナルコンピュータ１に送信し、処理は終了する。

【０３０４】以上のように、アダプタ２６は、暗号化されたソースプログラムを実行し、所定の場合、得られた結果を暗号化し、パーソナルコンピュータ１に送信する。

【０３０５】なお、オブジェクトプログラムを暗号化

し、暗号化されたオブジェクトプログラムをアダプタ２６が実行するようにしてもよい。図４４は、オブジェクトプログラムを暗号化する処理を説明するフローチャートである。ステップＳ５４１において、パーソナルコンピュータ１は、ソースプログラムをコンパイルし、所定のオブジェクトプログラムを生成する。ステップＳ５４２乃至ステップＳ５４６の処理は、図４２のステップＳ５０１乃至ステップＳ５０５とそれぞれ同様の処理なので、その説明は省略する。

【０３０６】図４５は、暗号化されたオブジェクトプログラムをアダプタ２６が実行する処理を説明するフローチャートである。ステップＳ５６１において、アダプタ２６のCPU３２は、パーソナルコンピュータ１から受信した、暗号化されたオブジェクトプログラムを、不揮発性メモリ３４に予め記憶されている認証局の公開鍵で復号する。ステップＳ５６２において、アダプタ２６のCPU３２は、復号されたオブジェクトプログラムをRAM３３に展開し、実行する。ステップＳ５６３乃至ステップＳ５６５は、図４３のステップ５２３乃至ステップＳ５２５とそれぞれ同様の処理なので、その説明は省略する。

【０３０７】次に、オブジェクトプログラムを暗号化する他の処理を、図４６のフローチャートを参照して説明する。ステップＳ５８１において、パーソナルコンピュータ１のCPU１１は、ソースプログラムをコンパイルし、オブジェクトプログラムを生成する。ステップＳ５８２において、パーソナルコンピュータ１のCPU１１は、インターフェース１７を介して、アダプタ２６にアプリケーション鍵Ｋａｐおよび個別鍵Ｋｉｄｖの発行を要求する。

【０３０８】ステップＳ５８３において、パーソナルコンピュータ１は、インターフェース１７を介して、アダプタ２６からアプリケーション鍵Ｋａｐおよび個別鍵Ｋｉｄｖ（アダプタ２６の不揮発性メモリ３４に記憶されている、アダプタ２６固有の鍵Ｋｓを基に、生成される）を受信する。ステップＳ５８４において、パーソナルコンピュータ１のCPU１１は、オブジェクトプログラムをアプリケーション鍵Ｋａｐで暗号化する。ステップＳ５８５において、パーソナルコンピュータ１のCPU１１は、コンテキストに含まれるマスター鍵K_{Mb}などを個別鍵Ｋｉｄｖで暗号化する。ステップＳ５８６において、パーソナルコンピュータ１のCPU１１は、アプリケーション鍵Ｋａｐで暗号化されたオブジェクトプログラム、および個別鍵Ｋｉｄｖで暗号化されたコンテキストに含まれるマスター鍵K_{Mb}などをHDD２１に記録させ、処理は終了する。

【０３０９】このように、パーソナルコンピュータ１は、アダプタ２６から供給されたアプリケーション鍵Ｋａｐおよび個別鍵Ｋｉｄｖで、オブジェクトプログラムおよびコンテキストを暗号化することができる。

【０３１０】図４６のフローチャートに示される手順で暗号化されたオブジェクトプログラムをアダプタ２６が実行する処理を、図４７のフローチャートを参照して説明する。ステップＳ６０１において、パーソナルコンピュータ１のCPU１１は、インターフェース１７を介して、アダプタ２６に、アプリケーション鍵Ｋａｐで暗号化されたオブジェクトプログラム、および個別鍵Ｋｉｄｖで暗号化されたコンテキストに含まれるマスター鍵K_{Mb}などを送信する。

【０３１１】ステップＳ６０２において、アダプタ２６のCPU３２は、不揮発性メモリ３４に予め記憶されている鍵Ｋｓおよびアプリケーション鍵Ｋａｐに、ハッシュ関数を適用し、個別鍵Ｋｉｄｖを生成する。ステップＳ６０３において、アダプタ２６のCPU３２は、受信したオブジェクトプログラムをアプリケーション鍵Ｋａｐで復号する。ステップＳ６０４において、アダプタ２６のCPU３２は、コンテキストに含まれるマスター鍵K_{Mb}などを個別鍵Ｋｉｄｖで復号する。

【０３１２】ステップＳ６０５において、アダプタ２６のCPU３２は、復号されたマスター鍵K_{Mb}などを含むコンテキストを利用して、オブジェクトプログラムを実行する。ステップＳ６０６乃至ステップＳ６０８の処理は、図４３のステップＳ５２３乃至ステップＳ５２５とそれぞれ同様なので、その説明は省略する。

【０３１３】以上のように、図４７のフローチャートで示される処理において、図４６のフローチャートで個別鍵Ｋｉｄｖを送信したアダプタ２６は、暗号化されたオブジェクトプログラムを実行することができる。従って、図４６のフローチャートで個別鍵Ｋｉｄｖを送信したアダプタ２６以外のアダプタは、オブジェクトプログラムを復号できるが、コンテキストを復号できず、暗号化されたオブジェクトプログラムは実行できない。

【０３１４】次に、アダプタ２６がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ１のCPU１１に実行させるときの処理を図４８のフローチャートを参照して説明する。ステップＳ６５１において、アダプタ２６のCPU３２は、オブジェクトプログラムの所定の命令列を、所定の規則に従って、変換する。

【０３１５】この変換は、例えば、ＤＥＳの暗号化または復号のプログラムの場合、Feistel構造などの基本構造を繰り返す処理のとき、いわゆるＦ関数で利用される４８ビットの拡大鍵と適切な乱数とに排他的論理和を所定の回数、適用するなどの変換を実行し、拡大鍵を解読しにくくする。また、例えば、ＤＥＳ　ＣＢＣ(Cipher Block Chaining)　Ｍｏｄｅで、多量のデータを復号するプログラムの場合、繰り返し構造の処理を順（シーケンシャル）に実行せず、多量のデータに対し、複数の繰り返し構造の処理を同時に実行し、拡大鍵を解読しにくくする。

【０３１６】また、例えば、ソースプログラムのインス

トラクションに対応するコード（例えば、加算を表すコードが”１”に対応し、乗算を表すコードが”２”に対応する）を毎回変更する。

【０３１７】ステップＳ６５２において、アダプタ２６のCPU３２は、変換された命令列を、インターフェース３１を介して、パーソナルコンピュータ１に送信する。

【０３１８】ステップＳ６５３において、パーソナルコンピュータ１のCPU１１は、デシャッフルされた命令列を実行する。ステップＳ６５４において、パーソナルコンピュータ１のCPU１１は、命令列を実行して得られた処理結果をアダプタ２６に送信する。

【０３１９】ステップＳ６５５において、アダプタ２６のCPU３２は、パーソナルコンピュータ１から受信した処理結果、およびアダプタ２６のCPU３２が算出し保持している計算結果を基に、処理を継続する。ステップＳ６５６において、アダプタ２６のCPU３２は、パーソナルコンピュータ１に処理を実行させるか否かを判定し、パーソナルコンピュータ１に処理を実行させないと判定された場合、処理は終了する。ステップＳ６５６において、パーソナルコンピュータ１に処理を実行させると判定された場合、手続きは、ステップＳ６５１に戻り、パーソナルコンピュータ１に処理を実行させる処理を繰り返す。

【０３２０】以上のように、アダプタ２６は、オブジェクトプログラムの処理の一部をパーソナルコンピュータ１に実行させることにより、高速にかつ安全に、オブジェクトプログラムの処理を実行することができる。

【０３２１】アダプタ２６は、オブジェクトプログラムに含まれる命令列を変換してパーソナルコンピュータ１に送信することにより、オブジェクトプログラムの解読が困難になる。アダプタ２６が、オブジェクトプログラムに含まれる命令列を暗号化して、パーソナルコンピュータ１に送信すれば、オブジェクトプログラムの解読は更に困難になる。

【０３２２】なお、図４６で説明したパーソナルコンピュータ１がアダプタ２６に供給するオブジェクトプログラムを暗号化する処理において、ソースプログラムに対しステップＳ６５１に示した変換を実行すれば、オブジェクトプログラムの解読は更に困難になる。

【０３２３】最後に、パーソナルコンピュータ１がEMDサーバ４から、事前に無料でダウンロードしたコンテンツを暗号化している暗号鍵をダウンロードするとともに、決済をする処理を、図４９のフローチャートを参照して説明する。ステップＳ６７１において、パーソナルコンピュータ１は、インターネット４を介して、EMDサーバ４と相互認証する。ステップＳ６７２において、パーソナルコンピュータ１のCPU１１は、インターネット接続インターフェース１１を介して、EMDサーバ４に、コンテンツの再生条件を示すデータを送信する。ステップＳ６７３において、EMDサーバ４は、受信した再生条件を示すデータを基に、支払い金額のデータをパーソナルコンピュータ１に送信する。

【０３２４】ステップＳ６７４において、パーソナルコンピュータ１のCPU１１は、EMDサーバ４から受信した支払い金額のデータをディスプレイ３に表示させる。ステップＳ６７５において、EMDサーバ４は、パーソナルコンピュータ１に、ユーザのクレジットカードの番号等の送信を要求する。ステップＳ６７６において、ユーザは、入力部２を操作し、パーソナルコンピュータ１にクレジットカードの番号等のデータを入力し、パーソナルコンピュータ１は、クレジットカードの番号等のデータをEMDサーバ４に送信する。

【０３２５】ステップＳ６７７において、EMDサーバ４は、パーソナルコンピュータ１から受信したクレジットカードの番号等のデータを基に、決済の処理を実行する。ステップＳ６７８において、EMDサーバ４は、インターネット４を介して、パーソナルコンピュータ１に所定の暗号鍵を送信する。ステップＳ６７９において、パーソナルコンピュータ１は、インターネット４を介して、EMDサーバ４から送信された所定の暗号鍵を受信し、処理は終了する。

【０３２６】以上のように、パーソナルコンピュータ１がEMDサーバ４から暗号鍵をダウンロードするとともに、EMDサーバ４は、決済の処理をすれば、パーソナルコンピュータ１がEMDサーバ４からコンテンツをダウンロードするとき、認証、暗号化、または決済などの処理が必要なくなるので、比較的大きなデータであるコンテンツを迅速にダウンロードすることができる。

【０３２７】以上においては、記録媒体として、ポータブルデバイス６を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。クレジットカードの番号等のデータを基に、決済の処理を実行するとして説明したが、ｓｍａｓｈ（商標）などの手続きにより、決済をするようにしてもよい。

【０３２８】また、図４９のフローチャートに示す処理の前に、パーソナルコンピュータ１とEMDサーバ４とが、例えば、ISO9798-3で規定されているhttp(Hypertext Transport Protocol)上のプロトコルを使用して、相互認証するようにしてもよい。

【０３２９】なお、ポータブルデバイス６は、予め個別鍵を記憶しているして説明したが、ユーザがポータブルデバイス６を購入後、EMDサーバ４などからダウンロードするようにしてもよい。

【０３３０】以上においては、記録媒体として、ポータブルデバイス６を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。

【０３３１】また、コンテンツは、曲のデータまたは音声データなどの楽音データ以外に、画像データ、その他

のデータとすることもできる。

【０３３２】以上のように、本発明によれば、次のような効果を奏することができる。

【０３３３】（１）　HDD２１に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上でHDD２１に記録するようにしたので、HDD２１に記録されているコンテンツをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

【０３３４】（２）　所定の曲を１回コピーしたとき、一定時間（上記例の場合、４８時間）の間、その曲をコピーすることができないようするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

【０３３５】さらにデータベースを更新する度に、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

【０３３６】（３）　外部の装置にコンテンツを渡したら、HDD２１上のコンテンツを消去するようにしたので、HDD２１内に元のデジタルデータであるコンテンツが残らず、その複製を大量に配布することが防止される。

【０３３７】（４）　HDD２１内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、HDD２１の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをHDD２１にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

【０３３８】（５）　パーソナルコンピュータ１が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

【０３３９】（６）　外部機器から、パーソナルコンピュータ１に対してデータを渡す前に、パーソナルコンピュータ１のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対してコンテンツを渡してしまうようなことが防止される。

【０３４０】（７）　曲の同一性の判定にISRCを用い、ISRCが取得できないときは、TOCを用いるようにしたので、ISRCが取得できなくとも、曲の同一性を判定することが可能になる。

【０３４１】（８）　パーソナルコンピュータ１におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ１に外付けされるアダプタ２６に負担させるようにしたので、パーソナルコンピュータ１のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

【０３４２】（９）　プログラムをプログラムに対応する鍵で暗号化し、プログラムの実行に必要なデータを、アダプタ２６が生成する固有の鍵で暗号化するようにしたので、プログラムのみをＣＤ－ＲＯＭなどの媒体で配布可能にしつつ、プログラムを他のアダプタ２６で実行することが防止される。

【０３４３】（１０）　音楽データなどのコンテンツを暗号化する鍵をダウンロードするとき、決済されるようにしたので、比較的大きなデータである音楽データなどのコンテンツを迅速にダウンロードすることができるようになる。

【０３４４】なお、アダプタ２６が実行する処理は、セキュアなプログラムでCPU１１が実行するようにしてもよい。この場合において、例えば、同一な値を有する保存用鍵は、保存用鍵が必要になった時点で、コンテンツ管理プログラム１１１により生成される。同様に、ハッシュ値は、コンテンツ管理プログラム１１１により隠蔽されて保存される。

【０３４５】また、アダプタ２６が実行する処理が、セキュアなプログラムでCPU１１により実行されるとき、パーソナルコンピュータ１は、アダプタ２６のRTC３５が供給する現在時刻に代えて、ネットワーク２に接続されている特定のサーバ（例えば、EMD登録サーバ３）から現在時刻のデータをダウンロードして、その現在時刻を基に、判定の処理を実行する。また、この場合において、パーソナルコンピュータ１は、所定の時間間隔で現在時刻を記憶して、記憶している時刻より以前の時刻が設定されたとき、エラーの表示を行い、時刻の設定を受け付けないようにしてもよい。

【０３４６】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【０３４７】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図２に示すように、磁気ディスク４１（フロッピディスクを含む）、光ディスク４２（CD-ROM(Compact Disc-Read Only Memory)、ＤＶＤ(Digital Versatile Disc)を含む）、光磁気ディスク４３（ＭＤ(Mini-Disc)を含む）、若しくは半導体メモリ４４などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM１２や、HDD２１などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部２５な

どのインタフェースを介して、ローカルエリアネットワークまたはインターネットなどのネットワーク２、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【０３４８】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０３４９】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０３５０】

【発明の効果】請求項１に記載の情報処理装置、請求項４に記載の情報処理方法、および請求項５に記載のプログラム格納媒体によれば、半導体ＩＣに実行させるプログラムに含まれる命令列が並び替えられ、プログラムが暗号化され、命令列が並び替えられ、暗号化されたプログラムが記録され、記録されているプログラムが、半導体ＩＣに送信されるようにしたので、記憶されているデータが不正に読み出され、解析されることを防止できるようになる。

【図面の簡単な説明】

【図１】本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。

【図２】パーソナルコンピュータ１の構成を説明する図である。

【図３】ポータブルデバイス６の構成を説明する図である。

【図４】パーソナルコンピュータ１の機能の構成を説明するブロック図である。

【図５】表示操作指示ウィンドウの例を示す図である。

【図６】録音プログラム１１３がディスプレイ２０に表示させるウィンドウの例を説明する図である。

【図７】コンパクトディスクからHDD２１にコンテンツをコピーする場合の処理を説明するフローチャートである。

【図８】図７のステップＳ１２の期限データベースチェック処理を説明するフローチャートである。

【図９】期限データベースの例を示す図である。

【図１０】ウォータマークを説明する図である。

【図１１】曲データベースの例を示す図である。

【図１２】HDD２１からポータブルデバイス６へコンテンツを移動する動作を説明するフローチャートである。

【図１３】HDD２１からポータブルデバイス６へコンテンツを移動する動作を説明するフローチャートである。

【図１４】HDD２１からポータブルデバイス６へコンテンツを移動する動作を説明するフローチャートである。

【図１５】図１２のステップＳ５５の選択されたコンテンツの再生条件などのチェック処理を説明するフローチャートである。

【図１６】ポータブルデバイス６が管理している再生条件を説明する図である。

【図１７】図１２のステップＳ５８のフォーマット変換処理の詳細を説明するフローチャートである。

【図１８】HDD２１からポータブルデバイス６へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図１９】HDD２１からポータブルデバイス６へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図２０】HDD２１からポータブルデバイス６へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図２１】ポータブルデバイス６からHDD２１へコンテンツを移動する場合の動作を説明するフローチャートである。

【図２２】ポータブルデバイス６からHDD２１へコンテンツをコピーする場合の動作を説明フローチャートである。

【図２３】EMDサーバ４からHDD２１へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図２４】図２３のステップＳ２０４の課金に関する処理の詳細を説明するフローチャートである。

【図２５】課金ログを説明する図である。

【図２６】図２のパーソナルコンピュータ１のIEC60958端子２４ａからHDD２１へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図２７】図２のパーソナルコンピュータ１のIEC60958端子２４ａからHDD２１へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図２８】HDD２１からIEC60958端子２４ａにコンテンツを出力する場合の動作を説明するフローチャートである。

【図２９】HDD２１からIEC60958端子２４ａにコンテンツを出力する場合の動作を説明するフローチャートである。

【図３０】図２８のステップＳ２７５の再生条件などのチェック処理を説明するフローチャートである。

【図３１】HDD２１からポータブルデバイス６経由でコンテンツを出力する場合の動作を説明するフローチャートである。

【図３２】HDD２１からポータブルデバイス６経由でコンテンツを出力する場合の動作を説明するフローチャートである。

【図３３】不揮発性メモリ３４の機能を説明する図である。

【図３４】アダプタ２６の動作を説明するフローチャートである。

【図３５】アダプタ２６の内部の構成を示す図である。

63

【図３６】不揮発性メモリ３４の内部の構成例を示す図である。

【図３７】不揮発性メモリ３４の内部の構成例を示す図である。

【図３８】ポータブルデバイス６とパーソナルコンピュータ１との相互認証の処理を説明するフローチャートである。

【図３９】ポータブルデバイス６とパーソナルコンピュータ１との相互認証の処理を説明するフローチャートである。

【図４０】ポータブルデバイス６とパーソナルコンピュータ１との相互認証の処理を説明するフローチャートである。

【図４１】ポータブルデバイス６とパーソナルコンピュータ１との相互認証の処理を説明するフローチャートである。

【図４２】ソースプログラムを暗号化する処理を説明するフローチャートである。

【図４３】暗号化されたソースプログラムをアダプタ２６が実行する処理を説明するフローチャートである。

【図４４】オブジェクトプログラムを暗号化する処理を説明するフローチャートである。

【図４５】暗号化されたオブジェクトプログラムをアダプタ２６が実行する処理を説明するフローチャートである。

【図４６】オブジェクトプログラムを暗号化する他の処理を説明するフローチャートである。

【図４７】暗号化されたオブジェクトプログラムをアダプタ２６が実行する他の処理を説明するフローチャートである。

【図４８】アダプタ２６がオブジェクトプログラムを実行する場合、処理の一部をパーソナルコンピュータ１のCPU１１に実行させるときの処理を説明するフローチャートである。

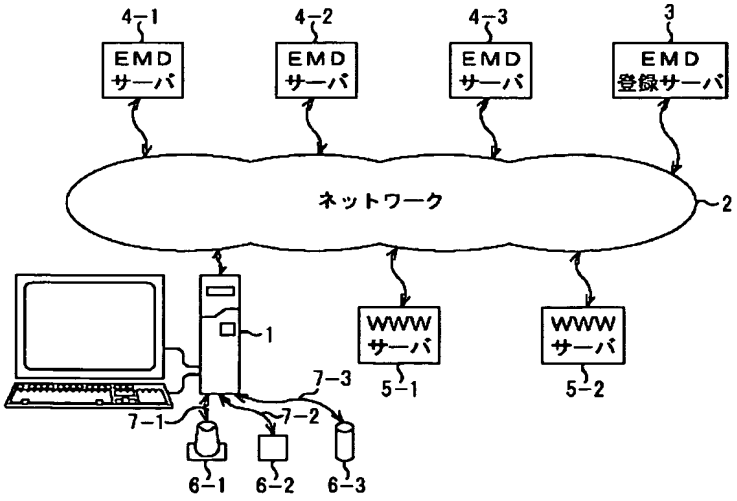
64

【図４９】パーソナルコンピュータ１がEMDサーバ４から暗号鍵をダウンロードするとともに、決済をする処理を説明するフローチャートである。

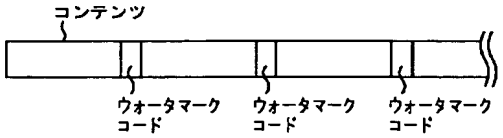
【符号の説明】

１　パーソナルコンピュータ，　２　ネットワーク，　３　EMD登録サーバ，　６－１乃至６－３　ポータブルデバイス，　１１　CPU，　１２　ROM，　１３RAM，　２１　HDD，　２４　音声入出力インターフェース，　２４ａ　IEC60958端子，　２６　アダプタ，　３２　CPU，　３３　RAM，　３４　不揮発性メモリ，　３５　RTC，　３６　ROM，　４１　磁気ディスク，　４２　光ディスク，４３　光磁気ディスク，　４４　半導体メモリ，　５３　CPU，　５４　RAM，５５　ROM，　５９　DSP，　６１　フラッシュメモリ，　１１１　コンテンツ管理プログラム，　１１２　表示操作指示プログラム，　１１３　録音プログラム，　１１４　コンテンツデータベース，　１３１　EMD選択プログラム，　１３２　チェックイン／チェックアウト管理プログラム，　１３３　コピー管理プログラム，　１３４　移動管理プログラム，　１３５　暗号方式変換プログラム，　１３６　圧縮方式変換プログラム，　１３７　暗号化プログラム，　１３８圧縮／伸張プログラム，　１３９　利用条件変換プログラム，　１４０　利用条件管理プログラム，　１４１　認証プログラム，　１４２　復号プログラム，１４３　PD用ドライバ，　１４４　購入用プログラム，　１４５　購入用プログラム，　１８１　フィルタリングデータファイル，　１８２　表示データファイル，　１８３　画像ファイル，　１８４　履歴データファイル，　３５１　保護アルミニュウム層，　３５２　電源パターン，　４０１－１乃至４０１－３配線

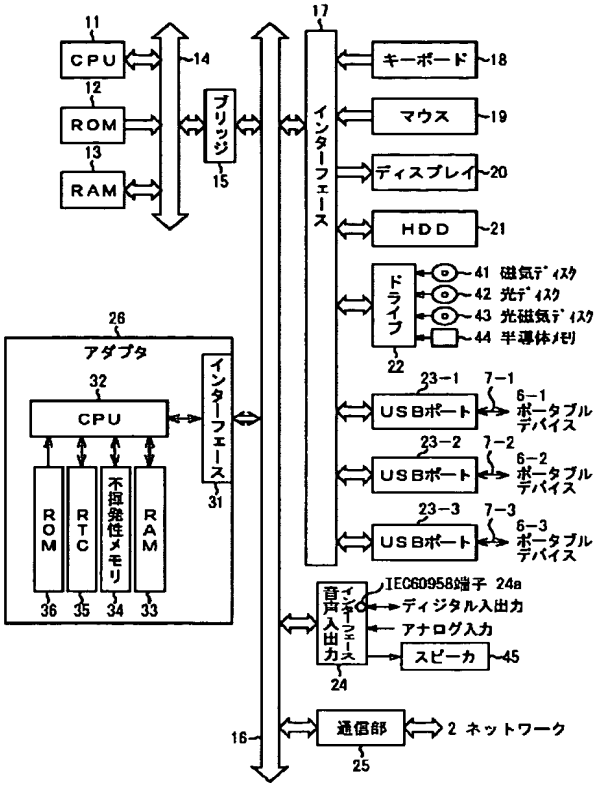
【図１】



【図１０】

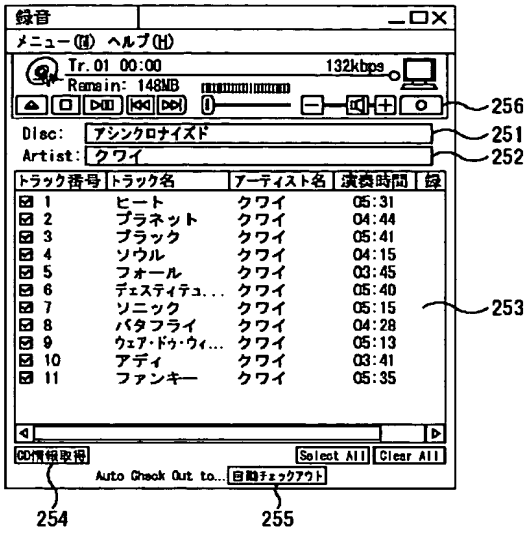


【図２】

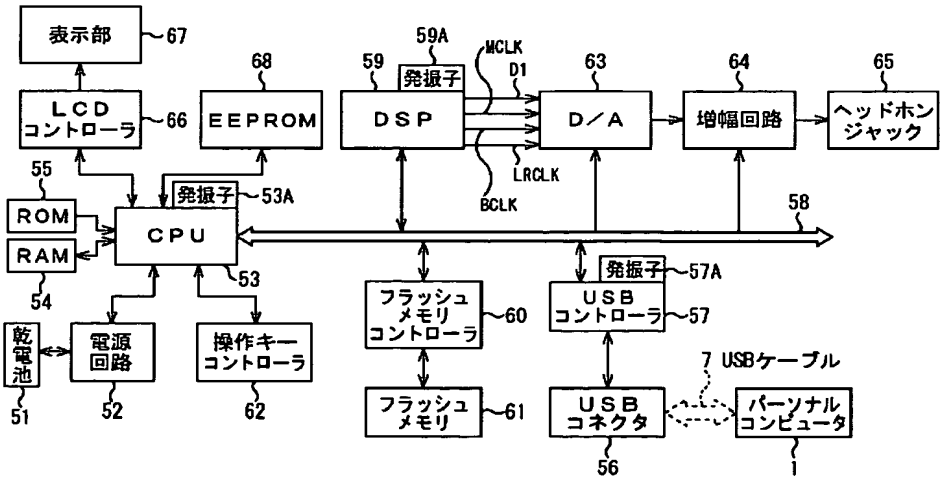


パーソナルコンピュータ 1

【図６】

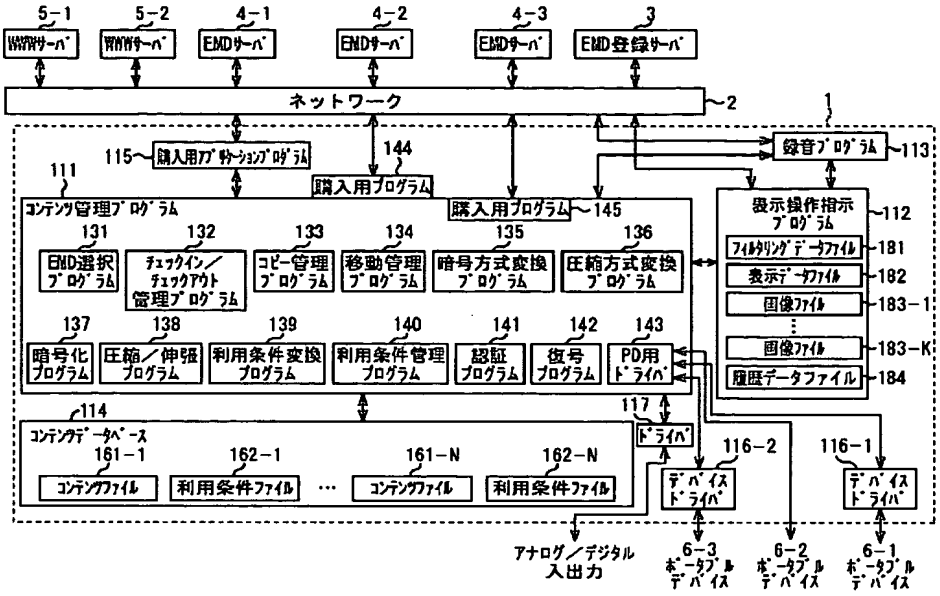


【図３】

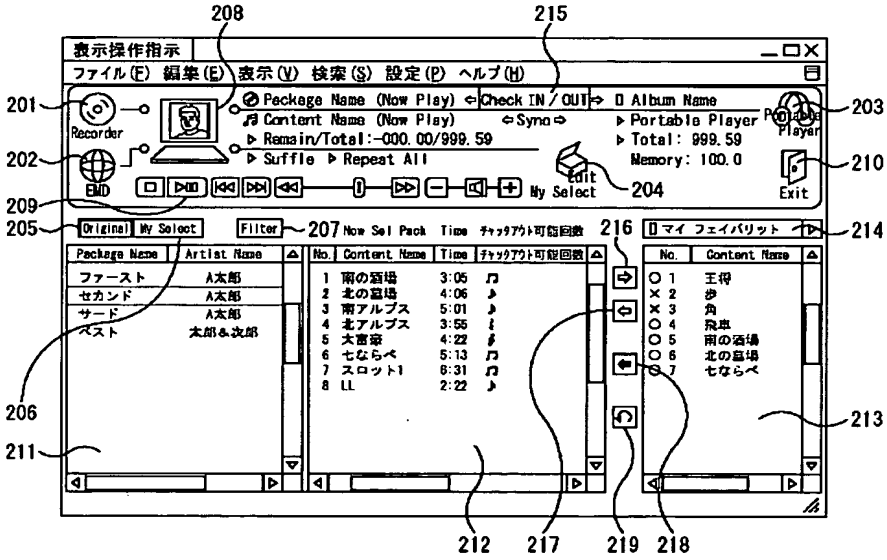


ポータブルデバイス 6

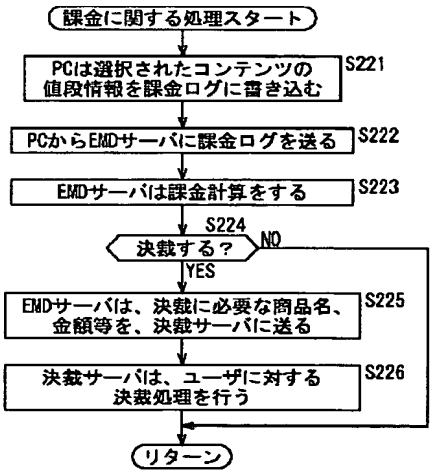
【図４】



【図５】



【図２４】



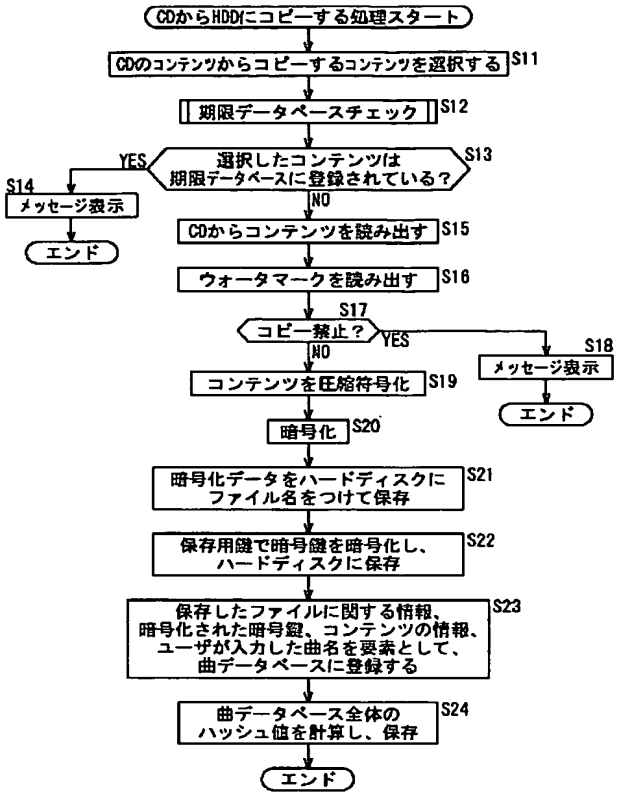
【図９】

期限データベース

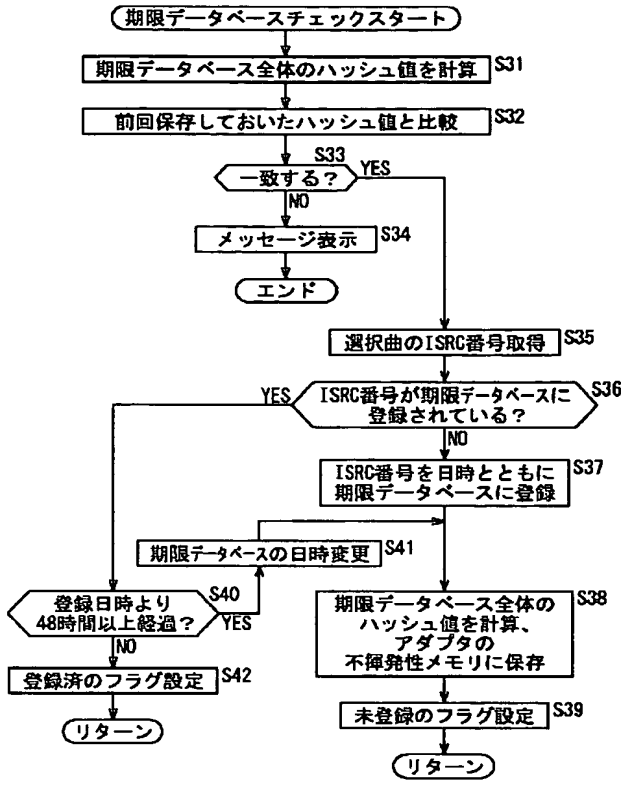
	アイテム1	アイテム2	アイテム3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

ハッシュ値	0xf3352e125934

【図７】



【図８】



【図１１】

曲データベース

	アイテム1	アイテム2	アイテム3	
ファイル名	xd000110.at2	px92341234.at2	aa0234287034.at2	
暗号化された暗号鍵	0xabababababab	0x9898989898989	0x123456789012	
曲名	春の小川	運命	荒城の月	
長さ	180	190	200	
再生条件:開始日時	-	2001.01.01.00:00	-	
再生条件:終了日時	1999.07.31.23:59	-	-	
再生条件:回数制限	-	20	-	
再生回数カウンタ	-	12	-	
再生時課金条件	-	-	¥5	
コピー条件:回数	2	0	0	
コピー回数カウンタ	1	0	0	
コピー条件:SCMS	0b01	0b10	0b00	

ハッシュ値	0xf9951e566321

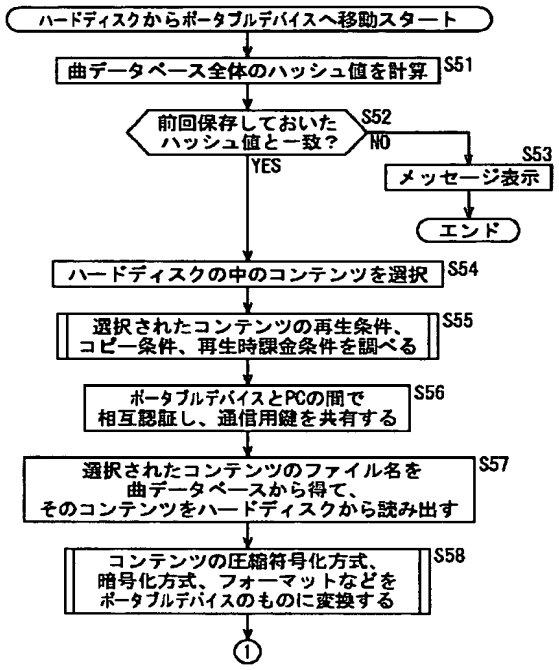
【図１６】

ポータブルデバイスが管理している再生条件

	アイテム1	アイテム2	アイテム3
コンテンツID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

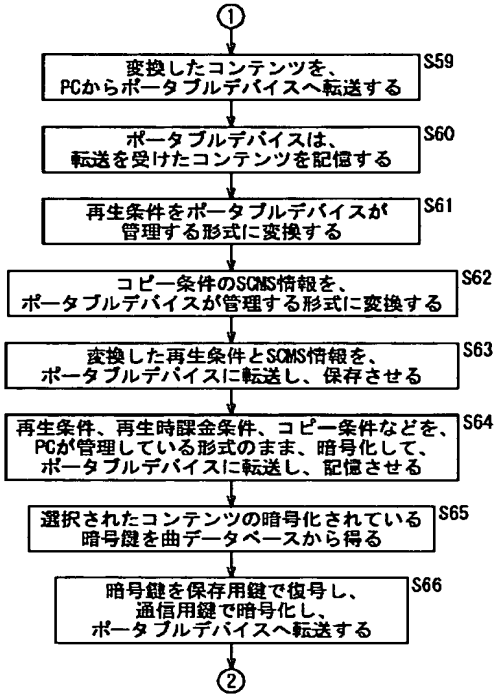
【図１２】

(12-1)



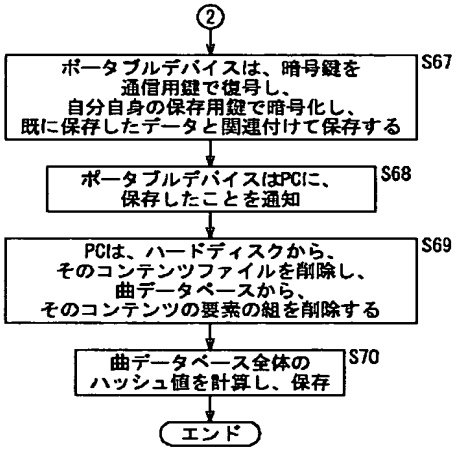
【図１３】

(12-2)

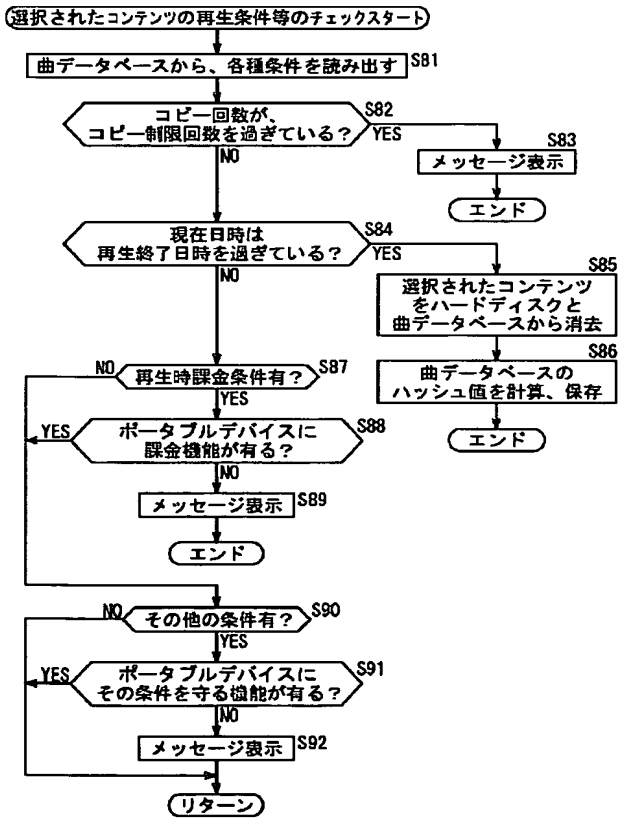


【図１４】

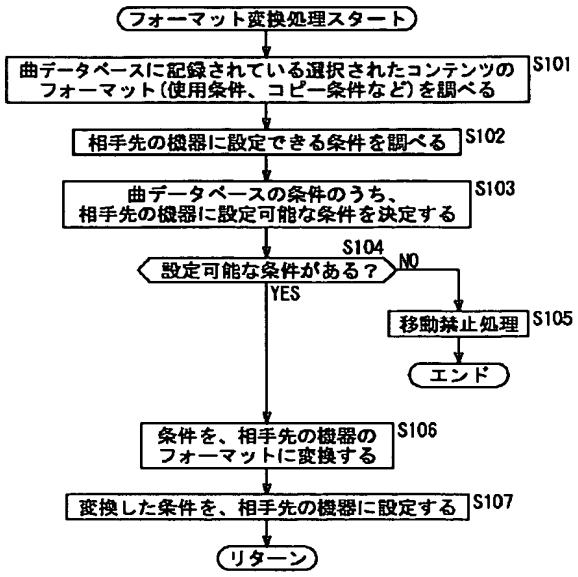
(12-3)



【図１５】

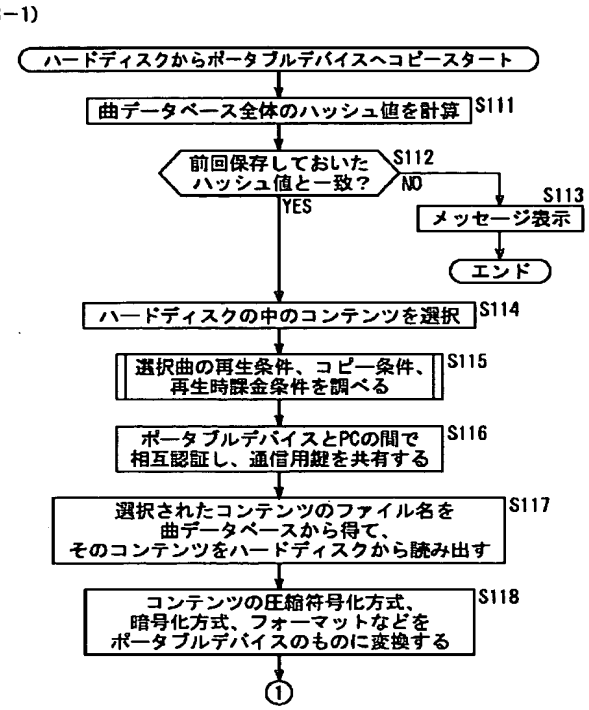


【図１７】



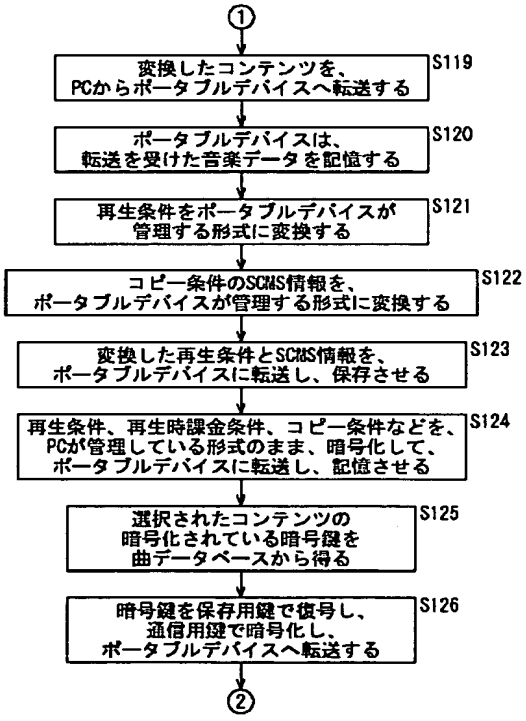
【図１８】

(18−1)



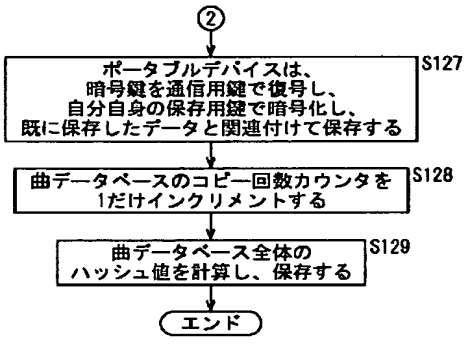
【図１９】

(18−2)

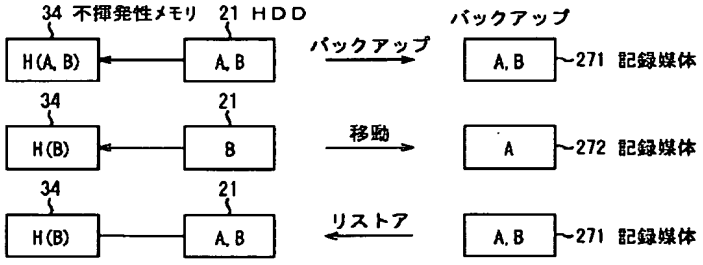


【図２０】

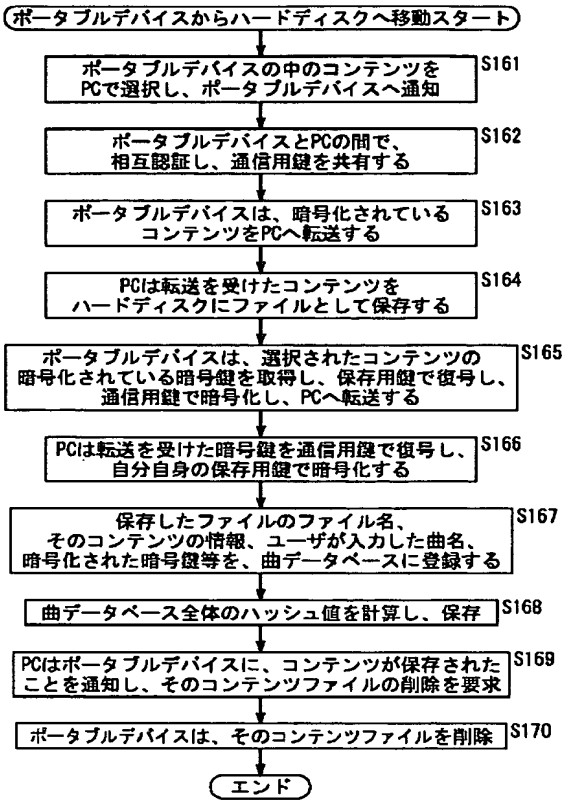
(18−3)



【図３３】

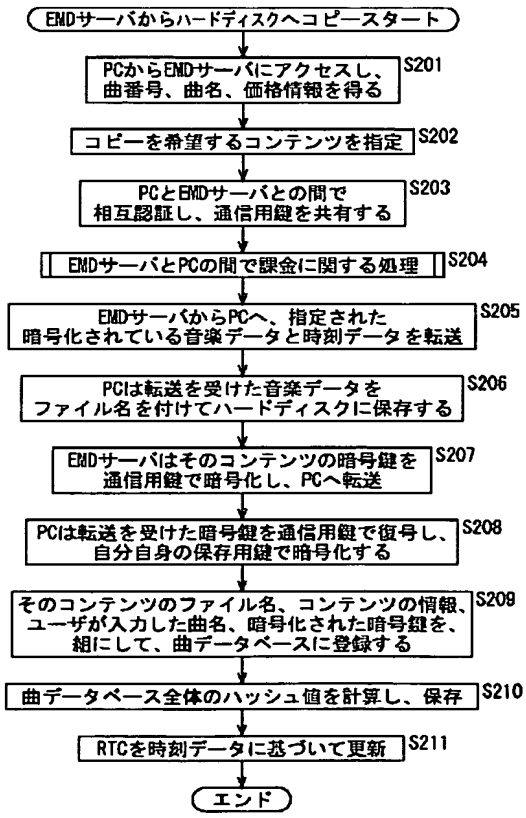


【図２１】

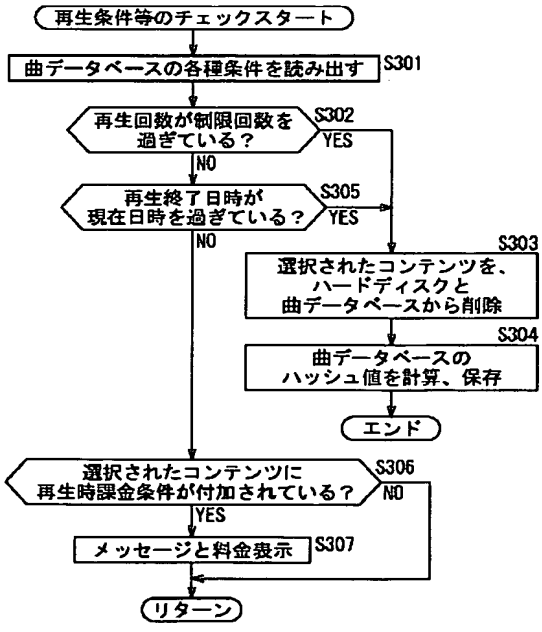


【図２２】

【図２３】



【図３０】



【図２５】

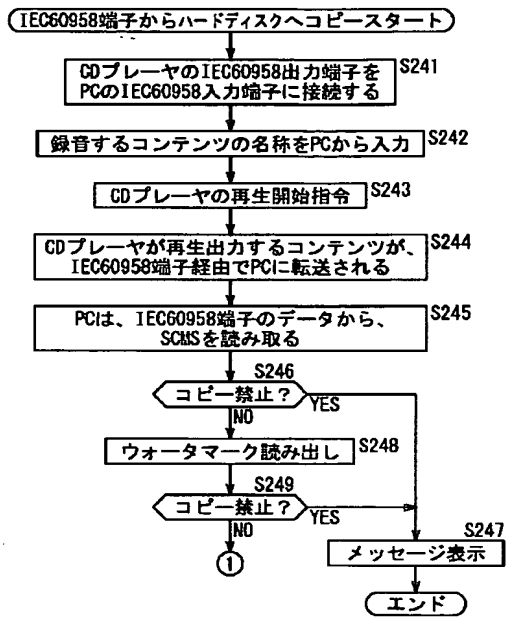
課金ログ

	アイテム1	アイテム2	アイテム3	
料金	50	50	60	

ハッシュ値	0xf8783e263517

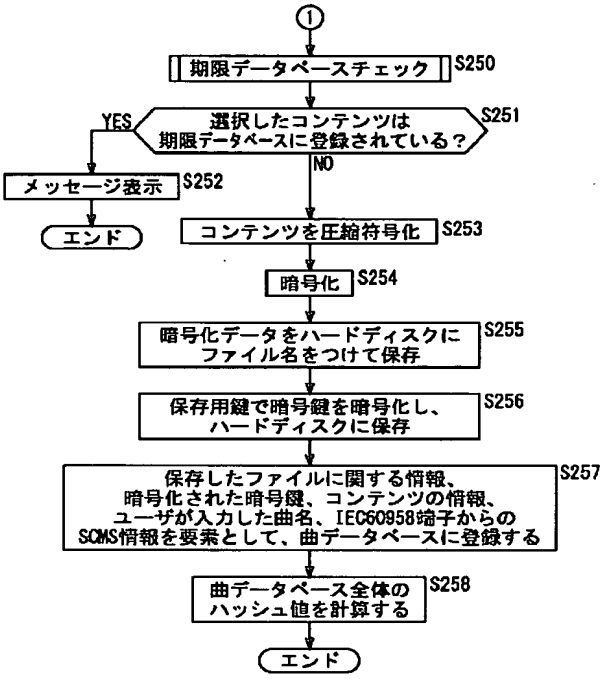
【図２６】

(26−1)



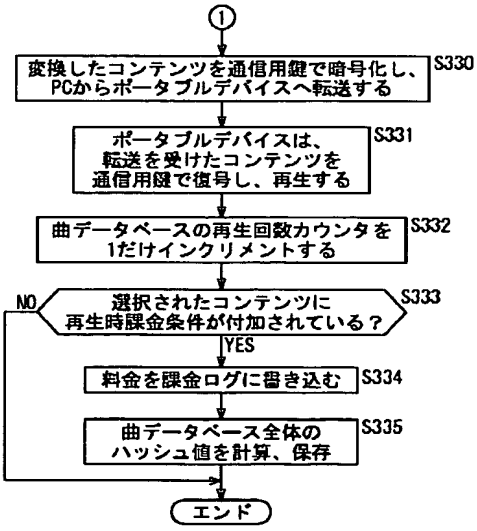
【図２７】

(26−2)

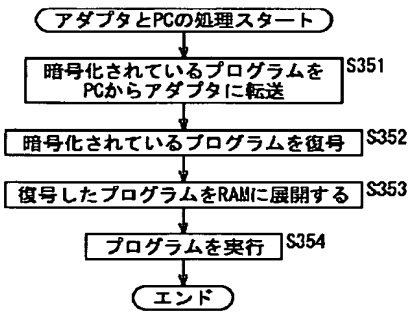


【図３２】

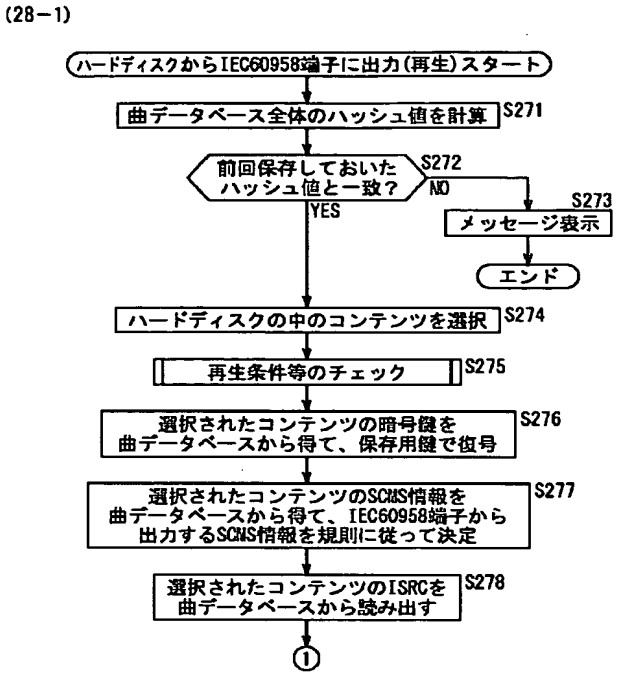
(31−2)



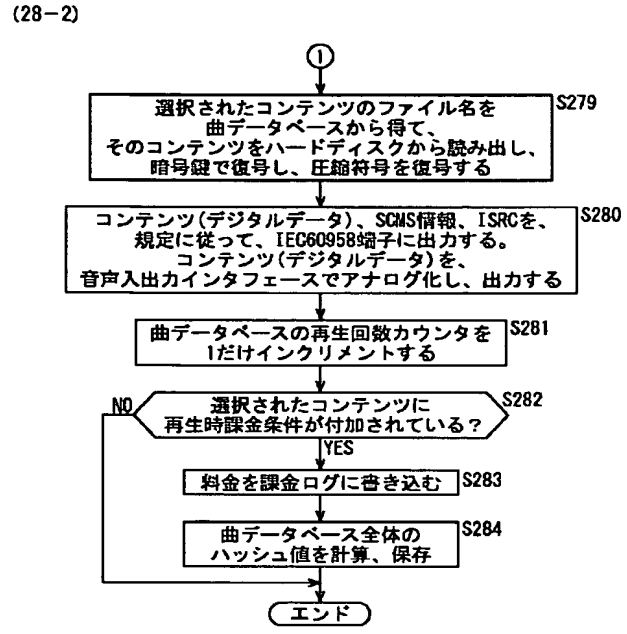
【図３４】



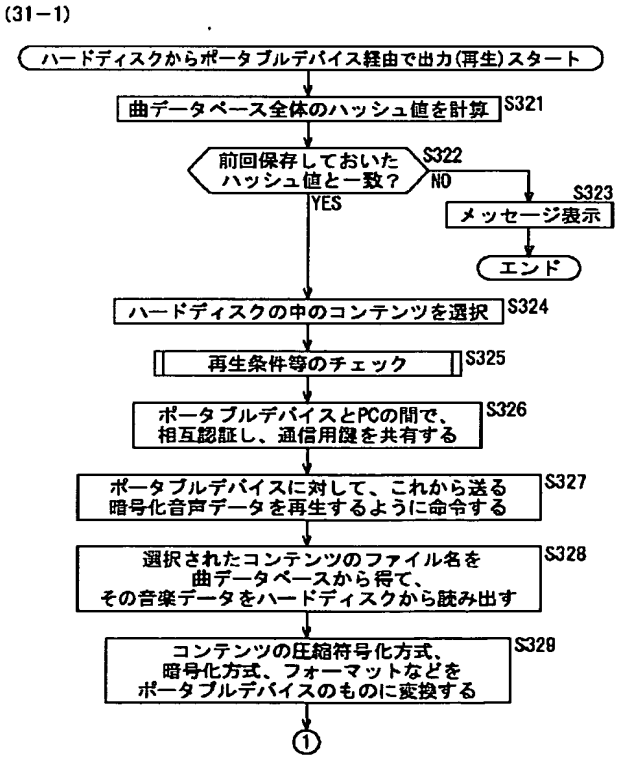
【図２８】



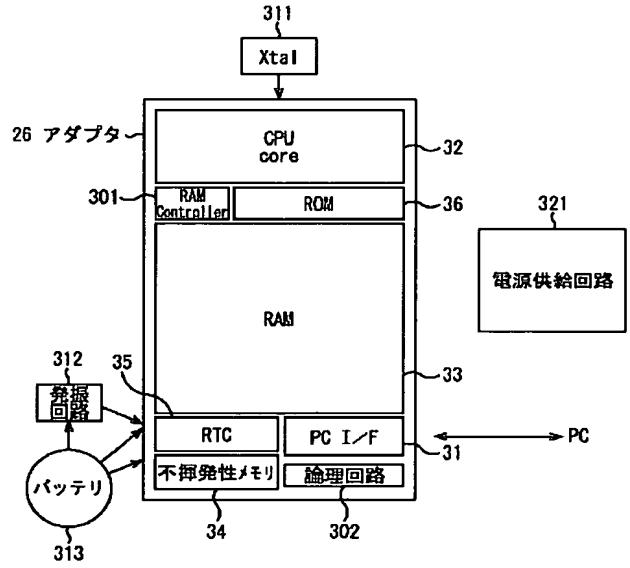
【図２９】



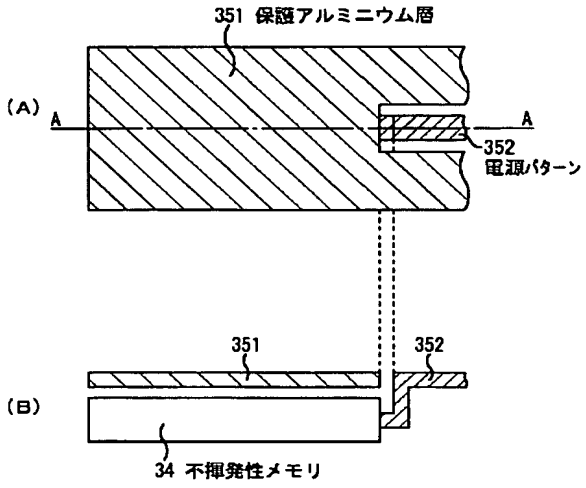
【図３１】



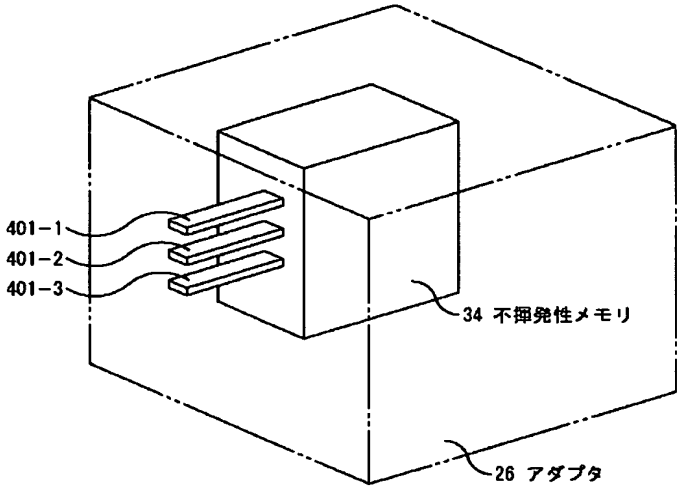
【図３５】



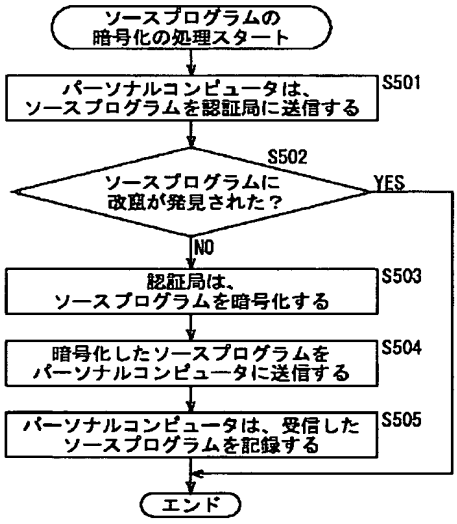
【図３６】



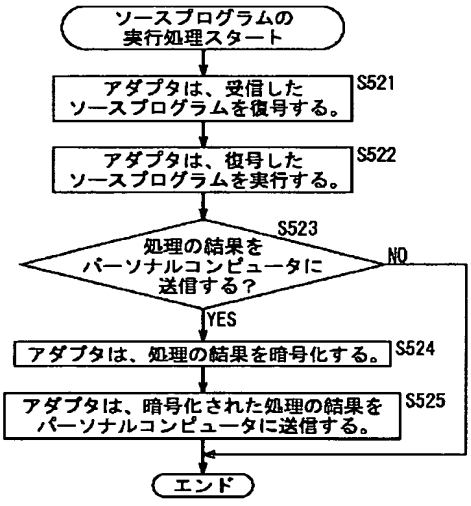
【図３７】



【図４２】

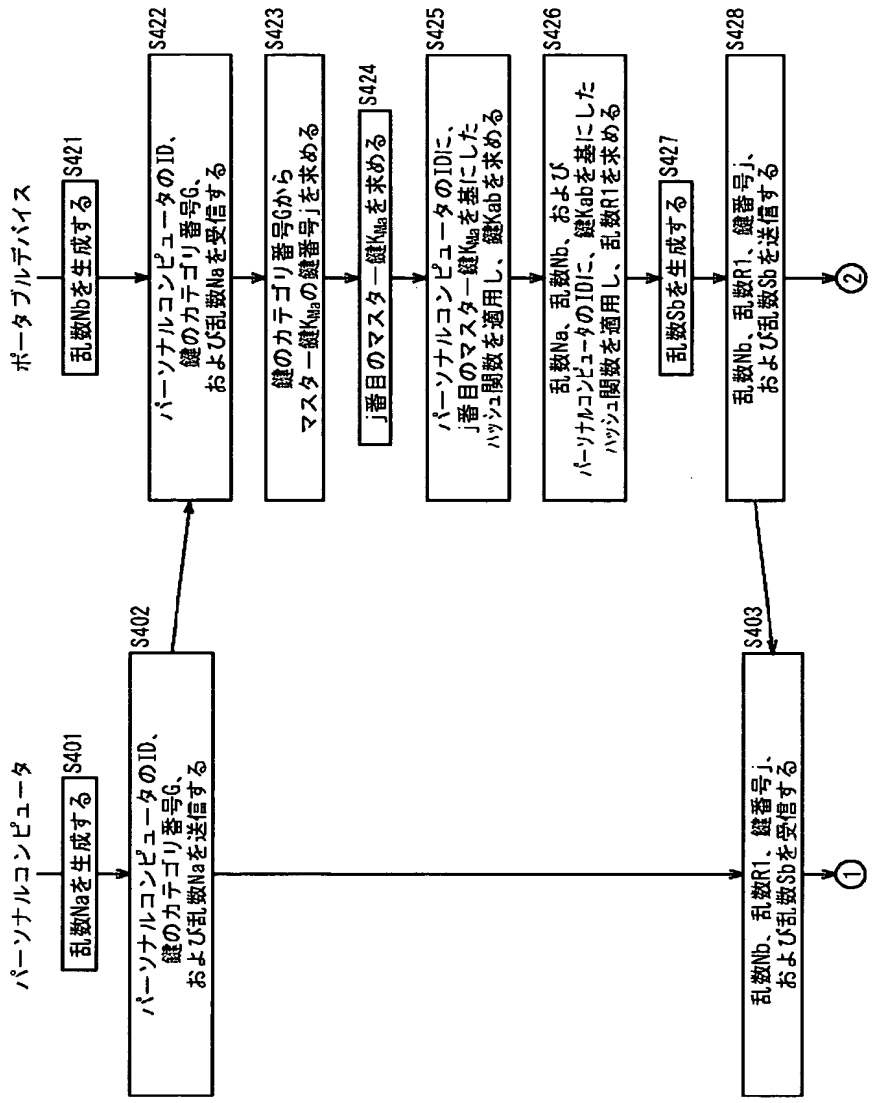


【図４３】



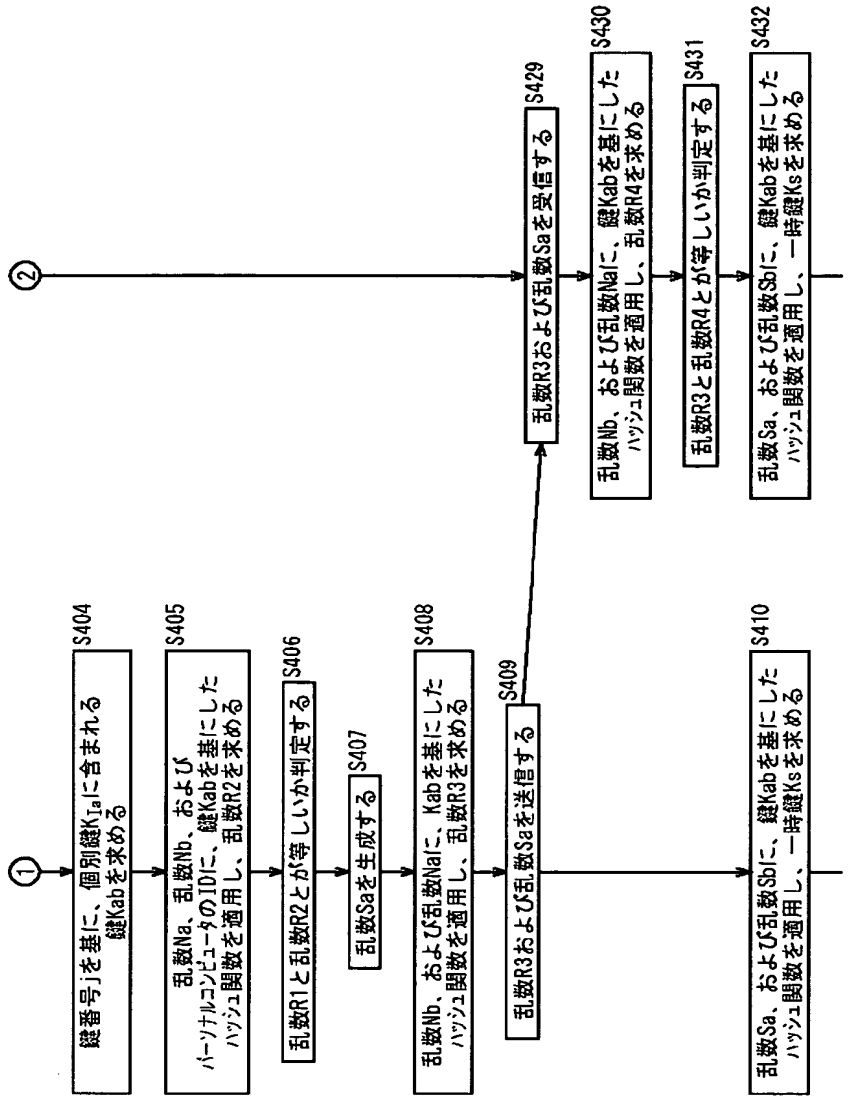
【図３８】

(38－1)


ポータブルデバイス
パーソナルコンピュータ
乱数Nbを生成する
S421
乱数Naを生成する
S401
パーソナルコンピュータのID、
鍵のカテゴリ番号G、
および乱数Naを受信する
S422
パーソナルコンピュータのID、
鍵のカテゴリ番号G、
および乱数Naを送信する
S402
鍵のカテゴリ番号Gから
マスター鍵Kmaの鍵番号jを求める
S423
j番目のマスター鍵Kmaを求める
S424
パーソナルコンピュータのIDに、
j番目のマスター鍵Kmaを基にした
ハッシュ関数を適用し、鍵Kabを求める
S425
乱数Na、乱数Nb、および
パーソナルコンピュータのIDに、鍵Kabを基にした
ハッシュ関数を適用し、乱数R1を求める
S426
乱数Sbを生成する
S427
乱数Nb、乱数R1、鍵番号j、
および乱数Sbを送信する
S428
乱数Nb、乱数R1、鍵番号j、
および乱数Sbを受信する
S403
①
②

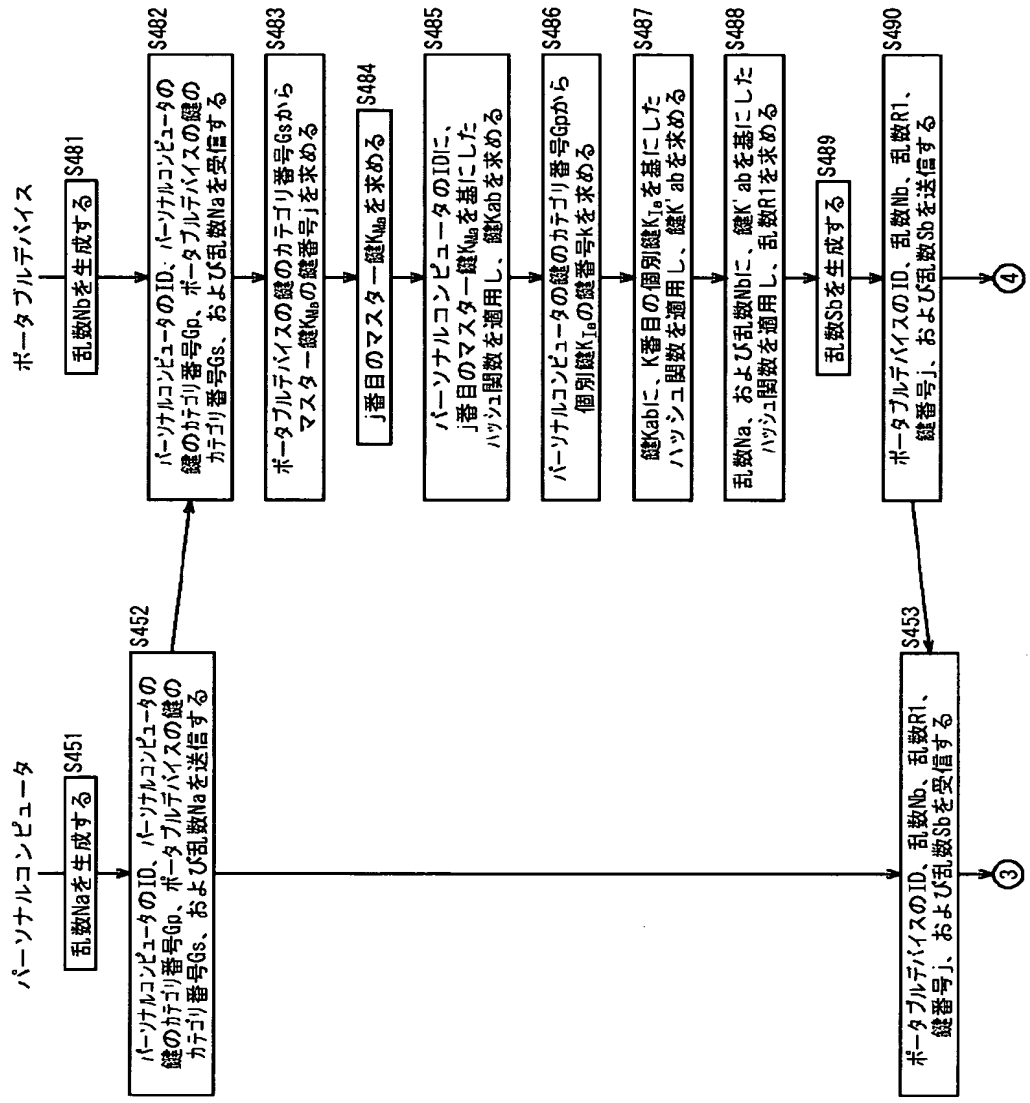
【図３９】

(38−2)


①
鍵番号jを基に、個別鍵K_{Ja}に含まれる鍵Kabを求める
S404
乱数Na、乱数Nb、およびパーソナルコンピュータのIDに、鍵Kabを基にしたハッシュ関数を適用し、乱数R2を求める
S405
乱数R1と乱数R2とが等しいか判定する
S406
乱数Saを生成する
S407
乱数Nb、および乱数Naに、Kabを基にしたハッシュ関数を適用し、乱数R3を求める
S408
乱数R3およびSaを送信する
S409
②
乱数R3およびSaを受信する
S429
乱数Nb、および乱数Naに、鍵Kabを基にしたハッシュ関数を適用し、乱数R4を求める
S430
乱数R3と乱数R4とが等しいか判定する
S431
乱数Sa、および乱数Sbに、鍵Kabを基にしたハッシュ関数を適用し、一時鍵Ksを求める
S432
乱数Sa、および乱数Sbに、鍵Kabを基にしたハッシュ関数を適用し、一時鍵Ksを求める
S410

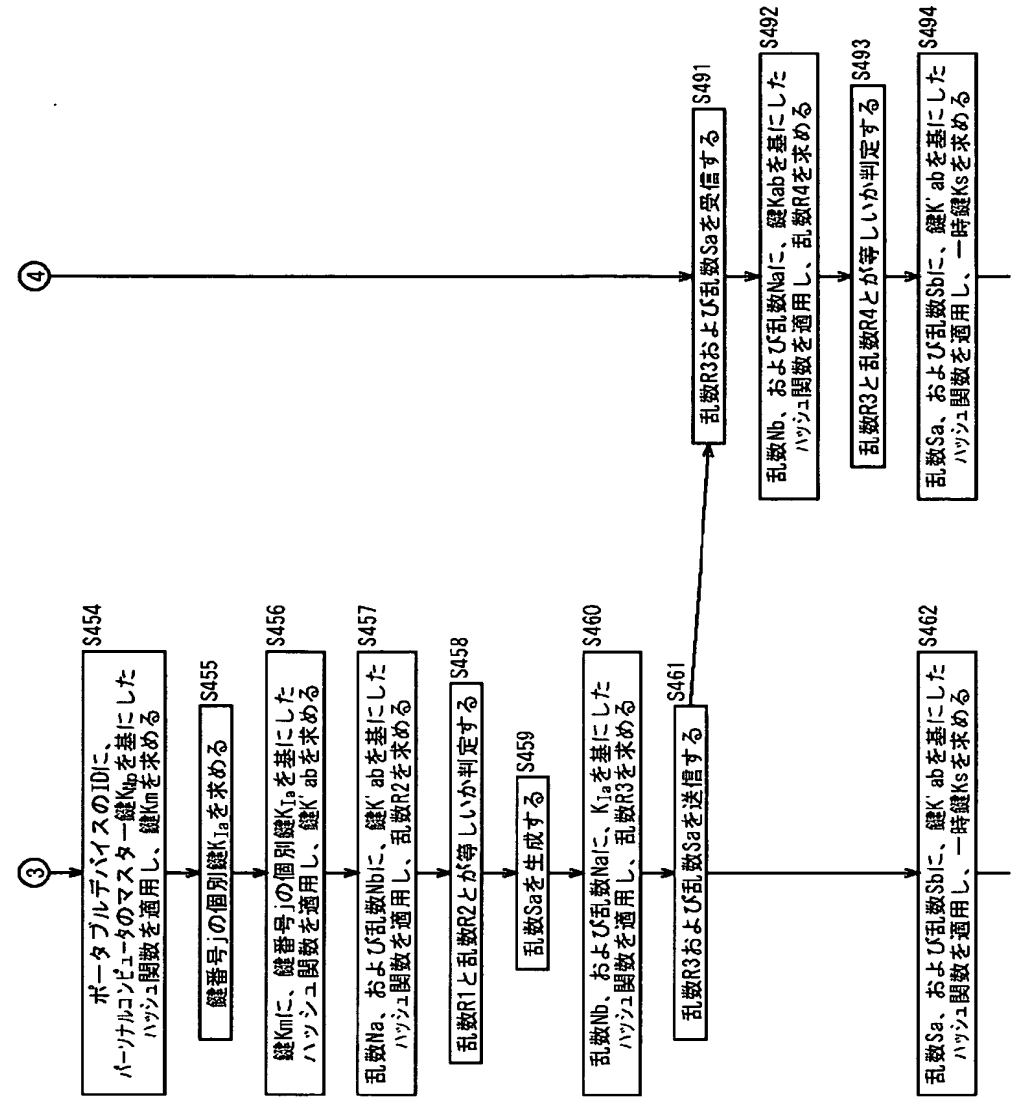
【図４０】

(40−1)

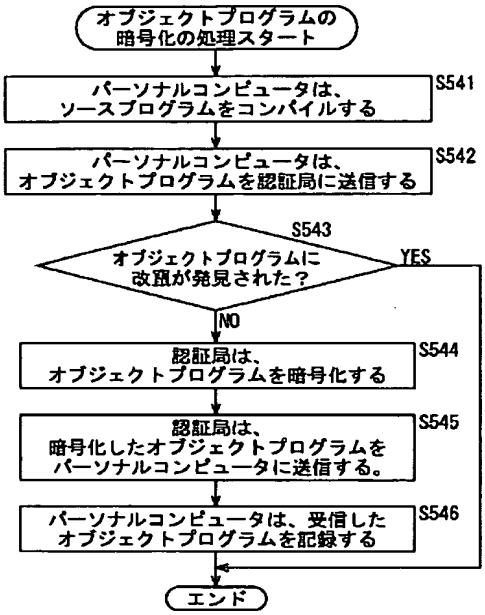

ポータブルデバイス
パーソナルコンピュータ
乱数Nbを生成する
S481
乱数Naを生成する
S451
パーソナルコンピュータのID、パーソナルコンピュータの鍵のカテゴリ番号Gp、ポータブルデバイスの鍵のカテゴリ番号Gs、および乱数Naを送信する
S452
パーソナルコンピュータのID、パーソナルコンピュータの鍵のカテゴリ番号Gp、ポータブルデバイスの鍵のカテゴリ番号Gs、および乱数Naを受信する
S482
ポータブルデバイスの鍵のカテゴリ番号Gsからマスター鍵K_{Ma}の鍵番号jを求める
S483
j番目のマスター鍵K_{Ma}を求める
S484
パーソナルコンピュータのIDに、j番目のマスター鍵K_{Ma}を基にしたﾊｯｼｭ関数を適用し、鍵Kabを求める
S485
パーソナルコンピュータの鍵のカテゴリ番号Gpから個別鍵K_{Ie}の鍵番号kを求める
S486
鍵Kabに、K番目の個別鍵K_{Ia}を基にしたﾊｯｼｭ関数を適用し、鍵K'abを求める
S487
乱数Na、および乱数Nbに、鍵K'abを基にしたﾊｯｼｭ関数を適用し、乱数R1を求める
S488
乱数Sbを生成する
S489
ポータブルデバイスのID、乱数Nb、乱数R1、鍵番号j、および乱数Sbを送信する
S490
④
パーソナルコンピュータのID、乱数Nb、乱数R1、鍵番号j、および乱数Sbを受信する
S453
③

【図４１】

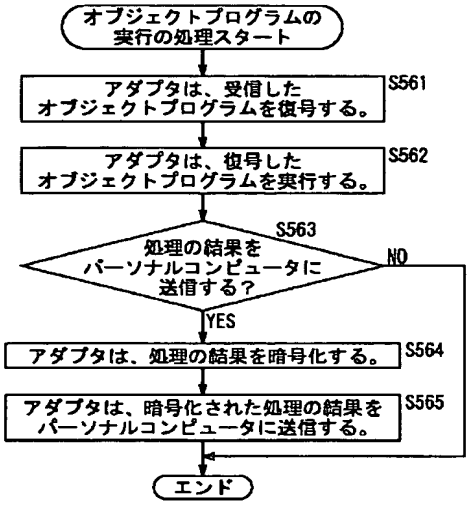
(40−2)


③
S454
ポータブルデバイスのIDに、パーソナルコンピュータのマスター鍵Kmbを基にしたハッシュ関数を適用し、鍵Kmを求める
S455
鍵番号jの個別鍵Kiaを求める
S456
鍵Kmに、鍵番号jの個別鍵Kiaを基にしたハッシュ関数を適用し、鍵K' abを求める
S457
乱数Na、および乱数Nbに、鍵K' abを基にしたハッシュ関数を適用し、乱数R2を求める
S458
乱数R1と乱数R2とが等しいか判定する
S459
乱数Saを生成する
S460
乱数Nb、および乱数Naに、Kiaを基にしたハッシュ関数を適用し、乱数R3を求める
S461
乱数R3およびSaを送信する
S462
乱数Sa、およびSbに、鍵K' abを基にしたハッシュ関数を適用し、一時鍵Ksを求める
④
S491
乱数R3およびSaを受信する
S492
乱数Nb、および乱数Naに、鍵Kabを基にしたハッシュ関数を適用し、乱数R4を求める
S493
乱数R3と乱数R4とが等しいか判定する
S494
乱数Sa、およびSbに、鍵K' abを基にしたハッシュ関数を適用し、一時鍵Ksを求める

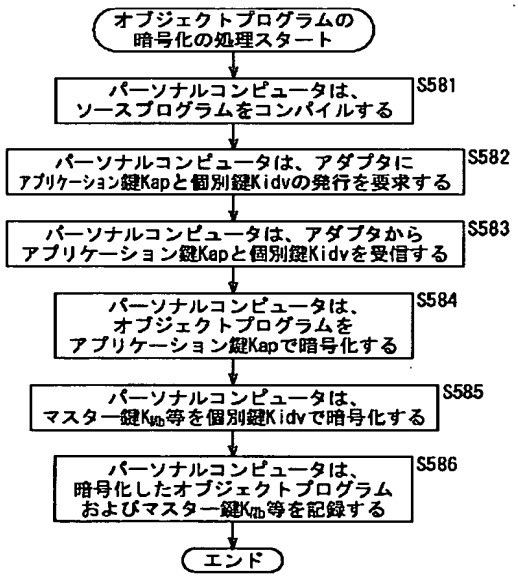
【図４４】



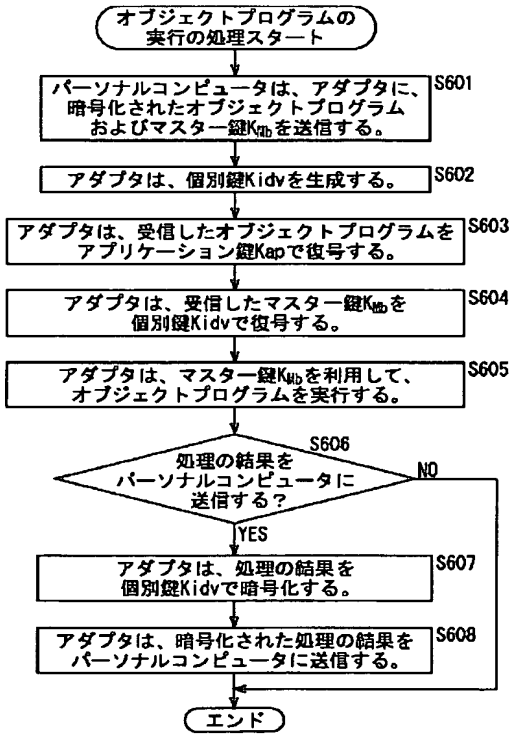
【図４５】



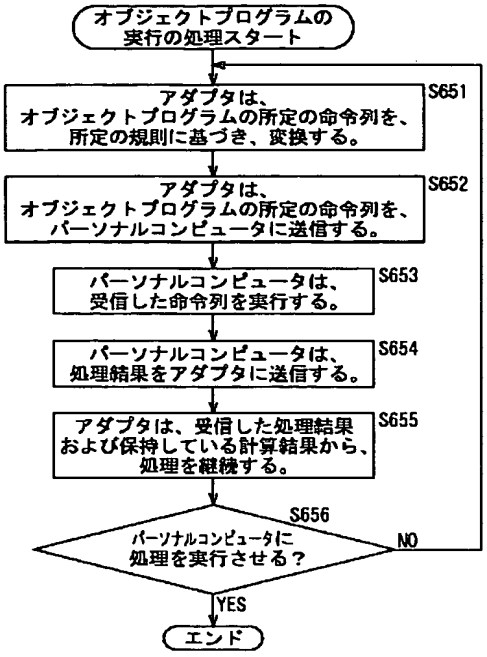
【図４６】



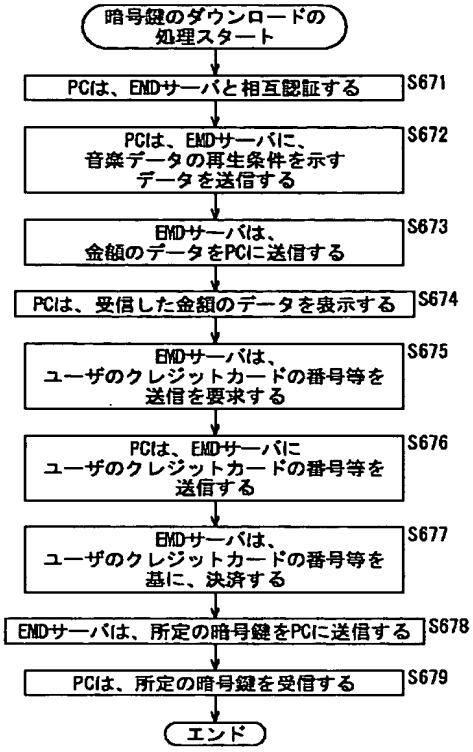
【図４７】



【図４８】



【図４９】



フロントページの続き

(72)発明者　田辺　充
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　江面　裕一
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　河原　博和
東京都品川区北品川６丁目７番35号　ソニー株式会社内